Klasifikasi Data

Adopsi Cloud yang Aman

Maret 2020

Pemberitahuan

Pelanggan bertanggung jawab untuk melakukan penilaian independen mereka terhadap informasi dalam dokumen ini. Dokumen ini: (a) adalah untuk tujuan informasi saja, (b) merupakan praktik dan penawaran produk AWS saat ini, yang dapat berubah tanpa pemberitahuan, dan (c) tidak memberikan komitmen atau jaminan apa pun dari AWS dan afiliasi, pemasok, atau pemberi lisensinya. Produk atau layanan AWS disediakan “sebagaimana adanya” tanpa garansi, representasi, atau kondisi apa pun, baik secara tersurat maupun tersirat. Tanggung jawab dan kewajiban AWS kepada pelanggan dikendalikan oleh perjanjian AWS, dan dokumen ini bukan bagian dari, juga tidak mengubah, perjanjian apa pun antara AWS dan pelanggannya.

Daftar Isi

Tinjauan Klasifikasi Data 1
Nilai Klasifikasi Data 1
Proses Klasifikasi Data 2
Model Klasifikasi Data yang Ada 3
Skema Klasifikasi Keamanan Nasional AS 4
Skema Kategorisasi Informasi AS 5
Skema Klasifikasi Data Britania Raya (UK) 5
Pertimbangan Pelanggan untuk Menerapkan Skema Klasifikasi Data 6
Pertimbangan Privasi dan Klasifikasi Data 7
Pertimbangan Baru dalam Klasifikasi Data 7
Rekomendasi AWS 8
Pendekatan Perusahaan 10
Memanfaatkan AWS Cloud untuk Mendukung Klasifikasi Data 12
Revisi Dokumen 14

Abstrak

Makalah ini menyediakan wawasan mengenai kategori klasifikasi data kepada organisasi publik maupun privat untuk dipertimbangkan saat memindahkan data ke cloud. Makalah ini menguraikan proses yang membuat pelanggan dapat membangun program klasifikasi data, berbagi contoh data dan kategori terkait yang mungkin termasuk di dalamnya, serta menguraikan praktik dan model yang saat ini diterapkan oleh penggerak pertama global dan pengadopsi awal bersama dengan klasifikasi data dan pertimbangan privasi. Makalah ini juga membahas cara implementasi program klasifikasi data yang dapat menyederhanakan penggunaan dan pengelolaan cloud, serta merekomendasikan agar pelanggan memanfaatkan standar dan kerangka kerja yang diakui secara internasional saat mengembangkan aturan klasifikasi data mereka sendiri.

Tinjauan Klasifikasi Data

Klasifikasi data adalah suatu langkah mendasar dalam pengelolaan risiko keamanan cyber. Ini melibatkan identifikasi jenis data yang sedang diproses dan disimpan dalam suatu sistem informasi yang dimiliki atau dioperasikan oleh suatu organisasi. Ini juga melibatkan pengambilan keputusan tentang sensitivitas data dan kemungkinan dampaknya jika data menghadapi gangguan, kehilangan, atau penyalahgunaan.

Untuk memastikan manajemen risiko yang efektif, organisasi harus bertujuan untuk mengklasifikasikan data dengan bekerja secara mundur dari penggunaan kontekstual data dan membuat skema kategorisasi yang memperhitungkan apakah kasus penggunaan tertentu menghasilkan dampak yang signifikan terhadap operasi organisasi (misalnya, jika data bersifat rahasia, perlu memiliki integritas, dan/atau tersedia).

> Sebagaimana yang digunakan dalam dokumen ini, istilah “klasifikasi” menyiratkan suatu pendekatan holistik termasuk taksonomi, skema, dan kategorisasi data untuk kerahasiaan, integritas, dan ketersediaan.

Nilai Klasifikasi Data

Klasifikasi data telah digunakan selama beberapa dekade untuk membantu organisasi membuat keputusan pengamanan data sensitif atau penting dengan tingkat perlindungan yang sesuai. Terlepas apakah data diproses atau disimpan di lokasi sistem atau cloud, klasifikasi data merupakan titik awal untuk menentukan tingkat pengendalian yang sesuai demi kerahasiaan, integritas, dan ketersediaan data berdasarkan risiko bagi organisasi. Misalnya, data yang dianggap “rahasia” harus diperlakukan dengan standar penanganan yang lebih tinggi dibandingkan data “publik” yang digunakan oleh masyarakat umum. Klasifikasi data memungkinkan organisasi mengevaluasi data berdasarkan sensitivitas dan dampak bisnis, sehingga membantu organisasi menilai risiko-risiko yang terkait dengan berbagai jenis data. Standar-standar organisasi, seperti Organisasi Standar Internasional (ISO) dan Institut Standar dan Teknologi Nasional (NIST), merekomendasikan skema klasifikasi data sehingga informasi dapat dikelola dan diamankan secara efektif berdasarkan tingkat kepentingan dan risiko yang terkait, menyarankan untuk menghindari praktik-praktik yang memperlakukan semua data secara setara. Setiap tingkat klasifikasi data harus dikaitkan dengan rekomendasi rangkaian dasar pengendalian data yang menyediakan perlindungan terhadap kerentanan, ancaman, dan risiko yang serupa dengan tingkat perlindungan yang ditentukan.

Mencatat risiko mengklasifikasi data secara berlebihan adalah hal yang sangat penting. Terkadang organisasi melakukan kesalahan dengan mengklasifikasikan secara luas kumpulan data yang berbeda pada tingkat sensitivitas yang sama. Klasifikasi yang berlebihan ini dapat menimbulkan biaya yang tidak beralasan dengan menerapkan kontrol dengan biaya tinggi yang dapat memengaruhi operasi bisnis. Pendekatan ini juga dapat mengalihkan perhatian ke kumpulan data yang kurang kritis dan membatasi penggunaan data oleh bisnis melalui persyaratan kepatuhan yang tidak perlu karena klasifikasi yang berlebihan.

Proses Klasifikasi Data

Pelanggan sering mencari rekomendasi yang nyata dalam hal menetapkan kebijakan klasifikasi data. Langkah-langkah ini berguna tidak hanya dalam fase pengembangan, tetapi dapat digunakan sebagai ukuran saat mengkaji kembali apakah kumpulan data sudah berada dalam kategori yang benar dengan perlindungan yang sesuai.

Paragraf di bawah ini memberikan pendekatan langkah bertahap, berdasarkan panduan yang diakui secara internasional yang dapat dipertimbangkan pelanggan saat mengembangkan kebijakan klasifikasi data[1][2]:

1. *Menyusun sebuah katalog data:* Melakukan inventarisasi dari beragam jenis data yang ada dalam organisasi, cara penggunaannya, dan jika ada data tersebut yang diatur oleh kebijakan atau regulasi kepatuhan. Setelah inventarisasi selesai, mengelompokkan jenis data menjadi salah satu tingkat klasifikasi data yang diadopsi organisasi.
2. *Menilai fungsi bisnis kritis dan melakukan sebuah penilaian dampak:* Suatu aspek penting dalam menentukan tingkat keamanan yang sesuai bagi kumpulan data adalah untuk memahami kekritisan data tersebut bagi bisnis. Setelah penilaian fungsi bisnis kritis, pelanggan dapat melakukan sebuah penilaian dampak pada setiap jenis data.
3. *Pelabelan informasi:* Melakukan penilaian jaminan kualitas untuk memastikan bahwa aset dan kumpulan data diberi label yang sesuai di bucket klasifikasinya masing-masing. Selain itu, mungkin perlu membuat label sekunder pada subjenis data untuk membedakan kumpulan data tertentu dalam suatu tingkatan karena privasi atau masalah kepatuhan lainnya. Penggunaan layanan seperti Amazon SageMaker dan AWS Glue memberikan wawasan dan dapat mendukung aktivitas pelabelan data.

[1] ISO 27001/27002 adalah standar keamanan global yang diadopsi secara luas yang menetapkan persyaratan dan praktik terbaik untuk pendekatan sistematis dalam mengelola informasi perusahaan dan pelanggan berdasarkan penilaian risiko berkala yang sesuai dengan skenario ancaman yang selalu berubah.

[2] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800 -60v1r1.pdf

4. *Pengelolaan aset:* Ketika kumpulan data diberi tingkat klasifikasi, data ditangani menurut pedoman penanganan yang sesuai untuk tingkat itu, yang mencakup kontrol keamanan khusus. Prosedur pengelolaan ini harus ditetapkan, tetapi juga menyesuaikan dengan perubahan teknologi. (Lihat "Pertimbangan Pelanggan untuk Menerapkan Skema Klasifikasi Data" di bawah untuk informasi tambahan mengenai pengelolaan data.
5. *Pemantauan berkelanjutan:* Terus melakukan pemantauan keamanan, penggunaan, dan pola akses sistem dan data. Hal ini dapat dilakukan melalui proses otomatis (lebih disukai) atau manual untuk mengidentifikasi ancaman eksternal, mempertahankan operasi sistem yang normal, menginstal pembaruan, dan melacak perubahan pada lingkungan.

Model Klasifikasi Data yang Ada

Amerika Serikat (A.S.) dan Britania Raya (UK) telah menetapkan skema klasifikasi data untuk data sektor publik. Kedua pemerintah itu menggunakan skema klasifikasi tiga tingkat dengan mayoritas data sektor publik diklasifikasikan dalam dua tingkat terbawah. Penting untuk diperhatikan bahwa bagi beberapa pemerintah, klasifikasi data yang lebih ekstensif mungkin berguna. Misalnya, kota Washington, D.C. di Amerika Serikat, telah membuat program klasifikasi data menggunakan skema klasifikasi lima tingkat yang dipuji secara luas oleh pendukung data terbuka, dan dapat menjadi model yang baik bagi pemerintah daerah lainnya. Skema klasifikasi data memiliki daftar pendek atribut dan ukuran atau kriteria terkait yang membantu organisasi menentukan tingkat kategorisasi yang sesuai.

Kota Washington, D.C. menerapkan kebijakan data baru pada tahun 2017 dengan berfokus pada transparansi, sambil tetap melindungi data sensitif. Meskipun Washington
D.C. menerapkan model lima tingkat, tingkatan ini dapat diselaraskan dengan skema klasifikasi tiga tingkat yang diadopsi secara luas dan digunakan dalam metode akreditasi cloud.[3]

Tingkat 0 — Data Terbuka. Data yang tersedia bagi masyarakat di kumpulan data dan situs web pemerintah yang terbuka.

Tingkat 1 — Data Publik, Tidak Dirilis secara Proaktif. Data tidak dilindungi dari pengungkapan publik atau tunduk pada penolakan berdasarkan hukum, peraturan, atau kontrak apa pun. Publikasi data di Internet publik berpotensi membahayakan keselamatan, privasi, atau keamanan siapa pun yang diidentifikasi dalam informasi tersebut.

[3] https://octo.dc.gov/page/district-columbia-data-policy

Tingkat 2 — Untuk Penggunaan Pemerintah Daerah. Data yang tidak terlalu sensitif dan dapat didistribusikan dalam pemerintahan tanpa batasan hukum, peraturan, atau kontrak. Data itu terutama data operasi bisnis harian pemerintah.

Tingkat 3 — Rahasia. Data yang dilindungi dari pengungkapan berdasarkan hukum, peraturan, atau kontrak dan yang sangat sensitif atau secara hukum, peraturan, atau kontrak dibatasi dari pengungkapan kepada lembaga publik lainnya. Data itu termasuk data terkait privasi (misalnya, informasi identitas pribadi (PII), informasi kesehatan yang dilindungi (PHI), standar keamanan data industri kartu pembayaran (PCI DSS), informasi pajak federal (FTI), dsb.)

Tingkat 4 — Rahasia Terbatas. Data yang apabila diungkapkan secara tidak sah akan berpotensi menyebabkan kerusakan atau cedera parah, termasuk kematian bagi mereka yang diidentifikasi dalam informasi, atau secara signifikan mengganggu kemampuan lembaga untuk menjalankan fungsi hukumnya.

Skema Klasifikasi Keamanan Nasional AS

Pemerintah AS menggunakan skema klasifikasi tiga tingkat untuk informasi keamanan nasional seperti yang dijelaskan dalam Perintah Eksekutif 135261. Skema ini difokuskan pada instruksi penanganan berdasarkan dampak potensial terhadap keamanan nasional apabila diungkapkan (yaitu bersifat rahasia).

1. Bersifat Rahasia — Informasi yang apabila terjadi pengungkapan yang tidak sah secara wajar dapat diperkirakan menyebabkan kerusakan pada keamanan nasional.

2. Rahasia — Informasi yang apabila terjadi pengungkapan yang tidak sah secara wajar dapat diperkirakan menyebabkan kerusakan parah pada keamanan nasional.

3. Sangat Rahasia — Informasi yang apabila terjadi pengungkapan yang tidak sah secara wajar dapat diperkirakan menyebabkan kerusakan yang sangat parah pada keamanan nasional.

Dalam tingkatan klasifikasi ini juga terdapat label sekunder yang dapat diterapkan sehingga memberikan informasi asal-usul dan dapat memodifikasi instruksi penanganan. AS juga menggunakan istilah "data tidak diklasifikasi" untuk merujuk pada data apa pun yang tidak dikelompokkan dalam tiga tingkat klasifikasi tersebut. Bahkan dengan data yang tidak diklasifikasi, ada potensi penggunaan label sekunder untuk informasi sensitif, seperti "Hanya Untuk Penggunaan Resmi" (FOUO) dan "Informasi Tidak Diklasifikasi yang Terkendali" (CUI) yang membatasi pengungkapan kepada publik atau personel yang tidak berwenang.

Skema Kategorisasi Informasi AS

Karena fokus sasaran dari sistem klasifikasi AS dan untuk mengatasi risiko tambahan terhadap informasi di luar kerahasiaan, NIST mengembangkan skema kategorisasi tiga tingkat berdasarkan potensi dampak terhadap kerahasiaan, integritas, dan ketersediaan informasi dan sistem informasi yang dapat digunakan untuk misi organisasi. Sebagian besar data yang diolah dan disimpan oleh organisasi sektor publik dapat dikategorikan sebagai berikut:

NIST mengembangkan skema kategorisasi tiga tingkat berdasarkan dampak potensial terhadap kerahasiaan, integritas, dan ketersediaan informasi dan sistem informasi.

• Rendah — dampak merugikan terbatas pada operasi organisasi, aset organisasi, atau individu.

• Sedang — dampak merugikan yang serius pada operasi organisasi, aset organisasi, atau individu.

• Tinggi — dampak merugikan yang parah atau bencana pada operasi organisasi, aset organisasi, atau individu.

Menurut data Tahun Fiskal 2015[4], departemen dan lembaga federal AS mengelompokkan 88 persen sistem mereka ke dalam kategori rendah dan sedang. AWS memiliki wilayah dan layanan yang diakreditasi untuk mendukung semua jenis kategori dan klasifikasi data.

Skema Klasifikasi Data Britania Raya (UK)

Pada tahun 2014, Britania Raya menyederhanakan skema klasifikasi datanya dengan mengurangi tingkatan dari enam menjadi tiga tingkat. Terdiri dari:

1. Resmi — Operasi dan layanan bisnis rutin, beberapa di antaranya dapat memiliki konsekuensi yang merusak jika hilang, dicuri, atau dipublikasikan di media, tetapi tidak ada yang mengalami peningkatan profil ancaman.

[4] https://www.gao.gov/assets/710/700588.pdf

2. Rahasia — Informasi sangat sensitif yang membenarkan tindakan perlindungan yang lebih tinggi untuk dilindungi dari pelaku ancaman yang sangat berkemampuan tinggi (misalnya, kompromi yang dapat secara signifikan merusak kemampuan militer, hubungan internasional, atau penyelidikan kejahatan terorganisir yang serius).
3. Sangat rahasia — Sebagian besar informasi sensitif yang membutuhkan tingkat perlindungan tertinggi dari ancaman paling serius (misalnya, kompromi yang dapat menyebabkan hilangnya nyawa secara luas atau dapat mengancam keamanan atau kesejahteraan ekonomi negara atau negara sahabat).

Menurut pengarahan inti kantor kabinet, pemerintah Inggris mengategorikan sekitar 90 persen datanya sebagai "Resmi" [5], yang berfungsi sebagai klasifikasi data tingkat dasar, diikuti dengan 'rahasia' dan 'sangat rahasia'. Inggris menggunakan pendekatan akreditasi yang tidak terpusat dan fleksibel dengan masing-masing lembaga menentukan layanan cloud yang sesuai untuk data "Resmi" berdasarkan jaminan keamanan penyedia layanan cloud (CSP) sesuai 14 prinsip keamanan cloud [6]. Sebagian besar lembaga pemerintah Inggris telah memutuskan bahwa menggunakan CSP yang memiliki reputasi dan skala besar saat menjalankan beban kerja dengan data "Resmi" adalah hal yang tepat.

Pertimbangan Pelanggan untuk Menerapkan Skema Klasifikasi Data

Selain menerapkan skema klasifikasi data, juga penting untuk menentukan peran penanganan data. ISO, NIST, dan standar lainnya menempatkan tanggung jawab klasifikasi data pada pemilik data, karena mereka berada pada posisi terbaik untuk menentukan nilai, penggunaan, sensitivitas, dan kekritisan datanya sendiri. Kewajiban manajemen risiko berbeda-beda tergantung peran pihak yang menangani data. Dengan kata lain, pemilik data (yaitu pengendali yang menghasilkan dan mengontrol konten, seperti instansi dan kementerian) dan bukan pemilik data (yaitu pengolah yang menangani data untuk menyediakan layanan) harus tunduk pada persyaratan yang sesuai untuk peran yang mereka mainkan. Dalam hal klasifikasi data sektor publik, departemen dan kementerian bekerja sebagai pemilik

[5] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/251481/Government - Security-Classifications-Supplier-Briefing-Oct-2013.pdf

[6] https://www.ncsc.gov.uk/collection/cloud-security?curPage=/collection/cloud-security/implementing-the-cloud-security-principles

data dan bertanggung jawab atas pengklasifikasian data mereka dan menentukan akreditasi keamanan yang diharapkan dapat dipenuhi oleh CSP mereka.

Penting untuk diperhatikan bahwa organisasi yang menerapkan tingkat klasifikasi tinggi yang menyeluruh untuk semua data (terlepas dari posisi risiko sebenarnya) tidak mencerminkan pendekatan keamanan berbasis risiko yang berfokus pada hasil. Melindungi data yang diklasifikasikan pada tingkat yang lebih tinggi memerlukan standar pemeliharaan yang lebih tinggi, yang berarti peningkatan pengeluaran pelanggan untuk mengamankan, memantau, mengukur, memulihkan, dan melaporkan risiko. Bagi data yang tidak memenuhi ambang batas yang disyaratkan, penggunaan sumber daya besar yang diperlukan untuk mengelola data berdampak tinggi secara aman adalah hal yang tidak praktis. Selain itu, kontrol tambahan yang ditempatkan pada data di tingkat klasifikasi yang lebih rendah dapat berdampak negatif terhadap ketersediaan, kelengkapan, atau ketepatan waktu data tersebut bagi tenaga kerja umum, pelanggan, dan/atau konstituen. Jika risiko dapat dikelola sehingga data ditangani pada tingkat klasifikasi yang lebih rendah, organisasi akan mengalami fleksibilitas paling tinggi dalam hal cara mereka menggunakan data tersebut.

Pertimbangan Privasi dan Klasifikasi Data

Klasifikasi data sangat penting karena undang-undang dan peraturan privasi global yang baru memberi hak untuk mengakses, menghapus, dan kontrol lain atas data pribadi kepada konsumen. Misalnya, berdasarkan Peraturan Perlindungan Data Umum Uni Eropa, organisasi diwajibkan untuk merespons permintaan konsumen tertentu dalam waktu satu bulan setelah diterimanya permintaan. Untuk merespons dengan tepat, organisasi umumnya harus memverifikasi identitas pemohon, menemukan data pribadi pemohon, memastikan data yang dikembalikan hanya berisi data pribadi pemohon, dan mungkin menolak permintaan jika tidak sesuai dengan hukum yang berlaku. Organisasi yang mengadopsi kebijakan klasifikasi data yang kuat memiliki posisi lebih baik untuk memberikan tanggapan yang tepat waktu bagi permintaan ini. Kerangka kerja klasifikasi data bersama dengan penandaan dan pelabelan yang tepat akan membantu melindungi data pribadi ini. Label sekunder dapat digunakan dalam tingkatan klasifikasi untuk membantu penandaan dan penemuan data privasi yang relevan. Hal ini memungkinkan organisasi untuk mengatasi masalah yang muncul dengan cepat. Mekanisme tambahan tersebut juga membantu dalam penelusuran dan pemantauan akses dari kumpulan data sensitif.

Pertimbangan Baru dalam Klasifikasi Data

Baik proses menuju cloud baru lahir atau sudah ditetapkan, sangat penting untuk

menetapkan aturan klasifikasi data. Mirip dengan meninjau praktik keamanan yang ada dan menetapkan kebijakan yang lebih baik berdasarkan ancaman yang lebih baru, pertimbangan tentang cara melindungi data diutamakan pada bagian ini sebagai contoh hal-hal yang harus dipertimbangkan pelanggan saat meninjau kembali kebijakan klasifikasi data yang ada. Baru-baru ini, percakapan dalam konsorsium industri telah mengangkat poin-poin berikut:

1. **Data tersebar di mana-mana:** Penggunaan teknologi modern di mana-mana dan ketergantungan pada informasi perusahaan pada semua sektor berarti volume data yang sangat besar disimpan, diproses, dan sedang transit di berbagai sistem, perangkat, dan pengguna akhir. Hal ini dapat menimbulkan tantangan yang signifikan bagi perusahaan yang bertanggung jawab untuk mengelola dan mengamankan data dalam jumlah besar.
2. **Ketergantungan intra dan antar organisasi:** Kebutuhan yang semakin meningkat untuk berkolaborasi dan berbagi informasi dalam suatu organisasi dan antar organisasi dalam sektor yang sama atau dengan kebutuhan misi yang serupa (misalnya, jaringan rumah sakit dan perawatan kesehatan).
3. **Pengetahuan pengguna akhir:** Model yang bergantung pada pengguna akhir untuk mengidentifikasi dan mengklasifikasi data, seperti data yang digunakan untuk proses pembelajaran mesin, bisa jadi rawan kesalahan dan seringkali tidak lengkap. Pengguna akhir mungkin kurang memiliki keterampilan atau kesadaran terhadap risiko untuk mengategorikan dan mengelola data secara efektif.
4. **Pengklasifikasi dan penandaan data:** Biasanya ada kekurangan definisi umum dan pemahaman tentang pengklasifikasi, serta kurangnya standar di seluruh industri atau berlanjutnya pelabelan
5. **Konteks:** Konteks bersifat penting. Sensitivitas dan kekritisan informasi yang sebenarnya sangat bergantung pada faktor-faktor lain, seperti bagaimana informasi itu digunakan dan dengan siapa, selain tentang perlunya informasi itu.

Meskipun tantangan ini mungkin bukan hal baru, semua itu adalah faktor yang perlu dipertimbangkan saat organisasi mengembangkan dan menerapkan klasifikasi data.

Rekomendasi AWS

Dalam kebanyakan kasus, AWS merekomendasikan untuk memulai dengan pendekatan klasifikasi data tiga tingkat (Tabel 1), yang telah terbukti cukup memenuhi kebutuhan dan persyaratan pelanggan publik dan komersial. Sebagai contoh, tabel di

bawah ini menyertakan tiga tingkatan dan aturan penamaan untuk setiap tingkatan. Untuk organisasi yang memiliki lingkungan data yang lebih kompleks atau jenis data yang bervariasi, pelabelan sekunder berguna tanpa menambahkan kerumitan dengan lebih banyak tingkatan. Kami merekomendasikan penggunaan jumlah tingkatan minimum yang wajar bagi organisasi.

Tabel 1: Cara klasifikasi data tiga tingkat

Klasifikasi Data	Kategorisasi Keamanan Sistem	Opsi Model Penerapan Cloud
Tidak diklasifikasikan	Rendah hingga Tinggi	Cloud publik terakreditasi
Resmi	Sedang hingga Tinggi	Cloud publik terakreditasi
Rahasia dan di atasnya	Sedang hingga Tinggi	Cloud publik atau cloud komunitas/hibrida/privat yang terakreditasi

Pertimbangan Residensi Data: AWS mendorong pelanggan untuk menilai pendekatan klasifikasi data mereka dan mempertajam data mana yang perlu tetap berada di dalam negara atau wilayah mereka, dan mengapa. Dengan demikian, pelanggan dapat menemukan bahwa data mereka, bahkan data yang berpotensi sensitif dan penting, dapat disimpan dan/atau direplikasi di tempat lain jika tidak ada persyaratan geografis hukum atau kebijakan tertentu. Hal ini nantinya dapat mengurangi risiko kerugian jika terjadi bencana dan memberikan akses pada teknologi dan kemampuan yang mungkin tidak tersedia di wilayah mereka. Pelajari lebih lanjut di laporan resmi Residensi Data AWS.

Skema klasifikasi data NIST telah dikenal luas dalam sertifikasi khusus sektor, secara nasional dan internasional. Faktanya, pemerintah seperti Filipina dan Indonesia sedang mengevaluasi dan mengadopsi skema klasifikasi data yang menerapkan prinsip serupa seperti model AS dan Inggris. Namun, organisasi berada pada posisi terbaik untuk mengembangkan skema klasifikasinya sendiri berdasarkan kebutuhan organisasi dan manajemen risiko. Organisasi yang ingin menghindari skema berjenjang yang berat dan lebih rumit dapat melaksanakan penilaian dampak risiko dan kemudian bergerak maju dengan skema berjenjang lebih sedikit yang lebih mudah dikelola dan diklasifikasi, seperti model tiga tingkat.

Organisasi harus memilih model penerapan cloud yang sesuai dengan kebutuhan spesifik mereka, jenis data yang mereka tangani, dan risiko yang ditaksir (lihat tabel di bawah).

Bergantung pada klasifikasi datanya, mereka perlu menerapkan kontrol keamanan yang relevan (misalnya, enkripsi) dalam lingkungan cloud mereka.

Saat menilai risiko dan menentukan kontrol keamanan, penting untuk memahami perbedaan layanan cloud komersial dari sistem lokal, perbedaan dalam implementasi kontrol (yaitu, model tanggung jawab bersama), dan kemungkinan adanya kontrol alternatif untuk dipertimbangkan dibandingkan dengan implementasi TI tradisional. Ketika organisasi telah sepenuhnya mengevaluasi cloud komersial dengan berbagai manfaat keamanan yang tersedia (misalnya, peningkatan ketersediaan dan ketahanan, peningkatan visibilitas dan otomatisasi, serta infrastruktur yang terus diaudit), mereka mungkin menemukan bahwa sebagian besar beban kerja mereka dapat disebarkan pada cloud dengan memperhatikan skema klasifikasi data, serupa dengan yang telah dilakukan pemerintah AS dan Inggris. Secara global, kami melihat organisasi sektor publik semakin memanfaatkan keuntungan keamanan asli dari cloud komersial serta memenuhi persyaratan keamanan dan kepatuhan mereka melalui klasifikasi data yang sesuai dan implementasi kontrol keamanan.

Ketika organisasi telah sepenuhnya mengevaluasi cloud komersial dengan berbagai manfaat keamanan yang tersedia, mereka mungkin menemukan bahwa sebagian besar beban kerja mereka dapat disebarkan pada cloud dengan memerhatikan skema klasifikasi data, serupa dengan yang telah dilakukan pemerintah AS dan Inggris.

Pendekatan Perusahaan

Bagian ini mengidentifikasi contoh khusus industri untuk klasifikasi data, yang mungkin mencakup persyaratan khusus sektor. Seperti yang telah disebutkan sebelumnya, jenis data yang berbeda (misalnya, data pemerintah, keuangan, dan perawatan kesehatan) mungkin memerlukan pertimbangan tambahan untuk tingkatan dan label sekunder dalam menangani prosedur penanganan yang berbeda. Terlepas dari data yang dimiliki oleh entitas publik atau komersial, pelanggan harus melakukan uji tuntas dengan mematuhi persyaratan peraturan dan kepatuhan lokal.

Bagan berikut berisi contoh skema klasifikasi data yang dipraktikkan saat ini, deskripsi tentang apa yang dapat dimasukkan dalam kategori tersebut berdasarkan tingkat, dan contoh jenis beban kerja untuk tingkat tertentu.

Contoh 1

Klasifikasi Data	Contoh Beban Kerja
Tingkat 3 – Data rahasia pemerintah dan sangat sensitif	Informasi keamanan dan pertahanan nasional Informasi intelijen pemerintah Informasi penegakan hukum Informasi investigasi pengawasan atau pemantauan program pemerintah
Tingkat 2 – Terlarang	Mengidentifikasi informasi pribadi tentang individu Manajemen Sumber Daya Manusia Informasi profil perorangan Kumpulan data pasar atau keuangan
Tingkat 1 – Data publik	Informasi pemasaran atau promosi Informasi terkait aktivitas program atau administratif pemerintah umum lainnya Manajemen dan pengembangan kebijakan tempat kerja intralembaga

Contoh 2

Klasifikasi Data	Contoh
Tingkat 3 – Sangat Strategis	Rahasia dagang yang sangat sensitif dan informasi bisnis rahasia material (misalnya, harga tertentu, informasi merger/akuisisi, rencana pemasaran, proses kepemilikan, rencana pemasaran, desain produk baru, penemuan sebelum permohonan paten atau disimpan sebagai rahasia dagang) yang pengungkapannya kepada publik dapat menyebabkan kerusakan hukum, keuangan, atau reputasi yang parah atau dahsyat.
Tingkat 2 – Terlarang	Sebagian besar data bisnis material dan non-material (misalnya, email, data akun penjualan dan pemasaran, kontrak yang dilaksanakan, tanda terima) Informasi yang diwajibkan oleh hukum untuk dilindungi dari pengungkapan yang tidak sah Catatan SDM karyawan (termasuk laporan pendisiplinan karyawan)

Tingkat 1 – Data terlindungi	Sistem CRM Nomor rekening bank vendor dan instruksi pembayaran Informasi yang tersedia hanya untuk sekelompok karyawan perusahaan tertentu yang digunakan untuk menjalankan bisnis Informasi untuk penggunaan internal saja

Memanfaatkan AWS Cloud untuk Mendukung Klasifikasi Data

Komputasi cloud dapat menawarkan kepada pelanggan kemampuan untuk mengamankan beban kerja mereka; baik di industri yang sangat diatur, sektor publik, atau usaha kecil-menengah, untuk memenuhi kebijakan dan persyaratan klasifikasi data. Penyedia layanan cloud (CSP), seperti AWS, menyediakan layanan standar berbasis utilitas yang disediakan sendiri oleh pelanggan. CSP tidak dapat melihat jenis data yang dijalankan pelanggan di cloud, yang berarti CSP tidak membedakan, misalnya, data pribadi dari data pelanggan lain saat menyediakan layanan cloud. Pelangganlah yang bertanggung jawab untuk mengklasifikasikan data mereka dan menerapkan kontrol yang sesuai dalam lingkungan cloud mereka (misalnya, enkripsi). Namun, kontrol keamanan yang diterapkan CSP dalam infrastruktur mereka dan penawaran layanan mereka dapat digunakan oleh pelanggan untuk memenuhi persyaratan data yang paling sensitif.

Layanan AWS menawarkan tingkat keamanan tinggi yang sama untuk semua pelanggan, terlepas dari jenis konten yang disimpan. AWS mengadopsi tingkat keamanan tinggi di semua layanan. Layanan ini kemudian diantrekan untuk sertifikasi terhadap keamanan internasional dan kepatuhan standar "emas", yang berarti pelanggan mendapatkan keuntungan dari tingkat perlindungan yang tinggi untuk data pelanggan yang diproses dan disimpan di cloud. Peristiwa risiko dan vektor ancaman yang menjadi perhatian terbesar sebagian besar diperhitungkan melalui disiplin ilmu kebersihan cyber yang mendasar (misalnya, sistem penambalan dan konfigurasi),

yang dapat ditunjukkan oleh CSP melalui sertifikasi keamanan yang diakui secara internasional dan diadopsi secara luas seperti ISO 27001 [7], Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS) [8], dan Kontrol Organisasi Layanan (SOC) [9]. Dalam mengevaluasi CSP, pelanggan harus memanfaatkan sertifikasi CSP ini sehingga pelanggan dapat dengan tepat menentukan apakah CSP (dan layanan dalam penawaran CSP) dapat mendukung persyaratan klasifikasi data mereka. Kami mendorong organisasi untuk menerapkan kebijakan yang mengidentifikasi sertifikasi cloud nasional, internasional, atau sektor tertentu yang ada dan pengesahan dapat diterima untuk setiap tingkat dalam skema klasifikasi data untuk menyederhanakan akreditasi dan mempercepat migrasi beban kerja ke cloud.

AWS menawarkan beberapa layanan dan fitur yang dapat memfasilitasi implementasi skema klasifikasi data oleh organisasi. Misalnya, Amazon Macie dapat membantu pelanggan menginventarisasi dan mengklasifikasikan data sensitif dan bisnis penting yang disimpan di AWS. Amazon Macie menggunakan pemelajaran mesin untuk mengotomatiskan proses menemukan, mengklasifikasikan, memberi label, dan menerapkan aturan perlindungan pada data. Hal ini membantu pelanggan lebih memahami lokasi penyimpanan informasi sensitif dan cara mengaksesnya, termasuk otentikasi pengguna dan pola akses.

Layanan dan fitur AWS lain yang dapat mendukung klasifikasi data termasuk, tetapi tidak terbatas pada:

- AWS Identity and Access Management (IAM) untuk mengelola kredensial pengguna, mengatur izin, dan memberi otorisasi akses.
- AWS Organizations membantu Anda mengatur lingkungan secara terpusat dengan pembuatan akun otomatis, pengelompokan akun untuk mencerminkan kebutuhan bisnis Anda, dan kebijakan untuk menegakkan tata kelola. Kebijakan dapat mencakup tindakan yang diperlukan seperti pemberian label pada sumber daya
- AWS Glue untuk menyimpan data dan menemukan metadata terkait seperti definisi tabel dan skema, di Katalog Data AWS Glue. Setelah dikatalogkan, data Anda segera dapat dicari dan tersedia untuk ETL.

[7] ISO 27001/27002 adalah standar keamanan global yang diadopsi secara luas yang menetapkan persyaratan dan praktik terbaik untuk pendekatan sistematis dalam mengelola informasi perusahaan dan pelanggan berdasarkan penilaian risiko berkala yang sesuai dengan skenario ancaman yang selalu berubah.

[8] Standar Keamanan Data Industri Kartu Pembayaran (juga dikenal sebagai PCI DSS) adalah standar keamanan informasi eksklusif yang dikelola oleh Dewan Standar Keamanan PCI (https://www.pcisecuritystandards.org/), yang didirikan oleh American Express, Discover Financial Services, JCB Internasional, MasterCard Worldwide, dan Visa Inc. PCI DSS berlaku untuk semua entitas yang menyimpan, mengolah, atau mentransmisikan kartu

[9] Laporan Kontrol Organisasi Layanan (SOC 1, 2, 3) dimaksudkan untuk memenuhi berbagai persyaratan audit keuangan untuk lembaga audit AS dan internasional. Audit untuk laporan ini dilakukan sesuai Standar Internasional untuk Keterlibatan Jaminan No. 3402 (ISAE 3402) dan Institut Akuntan Publik Bersertifikat di Amerika (AICPA): AT 801 (sebelumnya SSAE 16).

- Amazon Neptune, database grafik yang dikelola sepenuhnya, dapat memberi pelanggan wawasan tentang hubungan antara kumpulan data yang berbeda. Ini dapat mencakup identifikasi dan ketertelusuran data sensitif melalui analisis metadata.
- AWS KMS atau AWS CloudHSM untuk Manajemen kunci enkripsi dengan kunci yang dihasilkan AWS atau bawa kunci Anda sendiri (BYOK) dengan validasi FIPS 140-2.
- AWS CloudTrail untuk log ekstensif dalam melacak siapa, apa, dan kapan data dibuat, diakses, disalin/dipindahkan, dimodifikasi, dan dihapus.
- AWS Systems Manager untuk melihat dan mengelola operasi layanan seperti penambalan bersama dengan AWS Inspector untuk melakukan pemindaian kerentanan.
- AWS GuardDuty untuk deteksi ancaman intelijen yang mendukung persyaratan pemantauan berkelanjutan.
- AWS Config untuk mengelola perubahan konfigurasi dan menerapkan aturan tata kelola.
- AWS Web Application Firewall (WAF) dan AWS Shield untuk melindungi aplikasi web dari vektor serangan umum (misalnya, SQL Injection, Cross-Site Scripting, dan DDoS).

Untuk meninjau daftar lengkap layanan keamanan AWS, lihat Keamanan, Identitas, dan Kepatuhan di AWS.

Revisi Dokumen

Tanggal	Keterangan
Maret 2020	Diperbarui untuk mencerminkan layanan dan teknologi terkini.
Juni 2018	Publikasi pertama