Keamanan Data dan Kebocoran Data di Sektor Publik dan Swasta

Arsdiego Rahman Fadilla, Dwi Saptoaji, Firda Hasanah, Khezia Ichtus, dan Tom Hard Hasudungan

Teknologi Informasi/Universitas Bina Sarana Informatika
e-mail: arsdiego.rf@gmail.com
Teknologi Informasi/Universitas Bina Sarana Informatika
e-mail: dwisaptoaji10@gmail.com
Teknologi Informasi/Universitas Bina Sarana Informatika
e-mail: firdahasanah184@gmail.com
Teknologi Informasi/Universitas Bina Sarana Informatika
e-mail: heziap16@gmail.com
Teknologi Informasi/Universitas Bina Sarana Informatika
e-mail: tomhard512@gmail.com

Abstract

Nowadays people like to hacks public or private databases for various reasons, from political motivation to personal challenge or financial gain. These attacks can have serious consequences, ranging from financial loss and reputational damage to national security risks, which is why government's invest a lot of money in cybersecurity efforts.

That's why we need to be careful based on what application we use to prevent data leak from irresponsible person that breach the database for gaining money, because of that the goverment's need to increase bare minimum of data security on every application's that gonna be used, so everyone can use public or private application's without concerning any data leak.

This paper made us to know how important government's role to the national data security, hopefully by reading this journal people will understand why do we need government's part to increase our data security either on public or private database.

Keywords: database, data security, data breach

I. PENDAHULUAN

Proses digitalisasi merupakan salah satu kunci dari perkembangan revolusi industri yang ditandai dengan sengat eratnya kehidupan masyarakat dengan akses internet yang mudah.

Maka dari itu perkembangan teknologi dapat memudahkan masyarakat pada sektor-sektor tentu, salah satunya yaitu sektor kesehatan. Dengan adanya digitalisasi pada sektor kesehatan membuat petugas kesehatan dapat menyimpan database kesehatan menjadi lebih rapih, teratur, mudah, efektif dan efisien.

Tetapi tidak semuanya dapat berjalan dengan lancar, bahkan Badan Siber dan Sandi Negara (BSSN) menyatakan pada tahun 2020 terdapat peningkatan angka kejahatan *cybercrime* sebanyak empat kali lipat dari tahun 2019, dengan total 39 juta kasus. Tentunya hal itu dapat terjadi karena ada mekanisme yang kurang baik dari perlindungan data di Indonesia.

Maka dari itu pemerintah Indonesia menerbitkan peraturan perundang-undangan mengenai kehajatan cybercrime dan memperkuat hubungan kerjasama dengan Badan Siber dan Sandi Negara (BSSN) serta meningkatkan kerja sama dalam skala internasional untuk menangani ancaman cybercrime.

Salah satu Undang-Undang yang diterbitkan pemerintah adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Dalam Undang-Undang itu disebutkan bahwa setiap orang dilarang dengan sengaja mengakses komputer dan sistem elektronik dengan cara melanggar, menerobos, melampaui, menjebol sistem kemanan dan dapat dikenakan sanksi yang berat. Maka dari itu dalam penanganan *cybercrime* ini diperlukan kebijakan yang saling terintegrasi dan berkelanjutan.

II. KAJIAN LITERATUR

Untuk membahas jurnal ini lebih lanjut penting bagi kita untuk mengetahui dan memahami apa yang akan dibahas, agar lebih dapat memahami hal yang sedang dibahas tentang Keamanan Data dan Kebocoran Data.

Menurut ISO/IEC 27040, kebocoran data adalah kompromi keamanan yang menyebabkan data dilindungi terakses, diubah, hilang, atau diungkapkan tanpa izin. Maka dari itu keamanan data adalah tanggung jawab bersama yang memerlukan upaya berkelanjutan dan pendekatan yang komprehensif.

Keamanan data merujuk pada perlindungan terhadap data dari ancaman yang dapat merusak integritas, kerahasiaan, dan ketersediaan data tersebut. Dalam konteks ini, data yang dimaksud meliputi informasi pribadi, informasi perusahaan, data transaksi, dan data sensitif lainnya. Sedangkan kebocoran data (*data breach*) adalah kejadian yang terjadi ketika data yang sensitif, baik di sektor publik maupun swasta yang diakses, diungkapkan, atau disebarkan secara tidak sah.

Bahkan ada banyak penyebab kebocoran data, contohnya ialah:

- Sistem yang ketinggalan zaman
- Kebijakan kata sandi yang buruk
- Perangkat yang dicuri atau hilang
- Kerentanan perangkat lunak
- Kesalahan konfigurasi software
- Penipuan melalui rekayasa sosial (*social engineering)*
- Penggunaan kata sandi bawaan (*default password*)

Keamanan data di sektor publik melibatkan pengelolaan informasi yang diperoleh oleh lembaga pemerintah, yang mencakup data sensitif seperti identitas warga, data kesehatan, informasi pajak, dan catatan keuangan. Pentingnya perlindungan terhadap data ini terletak pada keberlanjutan kepercayaan publik terhadap pemerintah.

Beberapa tantangan utama di sektor publik seperti keterbatasan anggaran dan sumber daya karena ada banyak instansi pemerintah memiliki anggaran terbatas untuk mengembangkan dan memelihara sistem keamanan data yang canggi, lalu ada ancaman siber yang terus berkembang seperti serangan phishing, malware, ransomware, dan peretasan server menjadi ancaman serius bagi integritas data publik. Bahkan studi oleh Kwon et al. (2019) mengungkapkan bahwa meskipun banyak pemerintah di seluruh dunia telah mengimplementasikan kebijakan perlindungan data, masih banyak tantangan dalam penerapannya, seperti pengawasan yang lemah, kurangnya pelatihan, dan ketidakpastian regulasi.

Sedangkan di sektor swasta, perusahaan mengelola berbagai jenis data mulai dari data pelanggan, data transaksi, hingga informasi strategis yang sangat berharga. Keamanan data di sektor ini sangat krusial untuk menjaga reputasi perusahaan, menghindari kerugian finansial, dan mencegah pencurian identitas. Perusahaan di sektor swasta biasanya lebih mampu menginvestasikan dana yang lebih besar untuk memperkuat infrastruktur keamanan mereka. namun, mereka tetap menghadapi sejumlah tantangan seperti kepatuhan terhadap regulasi, serangan siber yang lebih canggih dan pengelolaan data yang lebih kompleks.

III. METODOLOGI PENELITIAN

Metode penelitian yang digunakan dalam penulisan ini adalah *digital research method*, yaitu studi penelitian yang pengumpulan datanya dilakukan secara daring. Riset berbasis digital tidak hanya terbatas pada penelitian yang mengeksplorasi fenomena online, tetapi juga memanfaatkan media daring dan teknologi digital dalam semua aspek penelitian. Riset berbasis digital dimaksudkan untuk memperoleh teori dan pengetahuan yang dapat menunjang penelitian.

IV. PEMBAHASAN

Karena proses digitalisasi sangat amat dibutuhkan di Indoneisa agar dapat mempercepat perkembangan revolusi industri 4.0, maka dari itu pemerintah menggunakannya sebagai sarana untuk mempermudah penginputan data. Tetapi kebocoran data menjadi kasus yang sulit untuk dihindarkan, seperti salah satu kasus pada bocornya data pada BPJS Kesehatan.

Badan Penyelenggaraan Jamninan Sosial (BPJS) Kesehatan adalah salah satu Badan Hukum Milik Negara yang memiliki fungsi untuk menyelenggarakan program jaminan kesehatan bagi masyarakat Indonesia yang berada di Indonesia. Bahkan pada tahun 2022 diproyeksikan jumlah peserta BPJS Kesehatan mencapai angka 245.144.462 jiwa atau setara dengan 88.51% dari total seluruh populasi rakyat di Indonesia.

Pada akhir Mei 2021, telah terungkap kasus kebocoran data berupan Nomor Induk Kependudukan (NIK), nama, alamat, nomor telepon, data tanggungan, status pembayaran dan masih banyak yang lainnya. Data-data tersebut identik dengan data yang dikelola oleh BPJS Kesehatan. Kasus tersebut terungkap ketika sebuah akun bernama Kotz menawarkan 279 juta salinan data warga Indonesia ke dalam sebuah forum *online* bernama *Raid* Forums. Karena itu Direktorat Tindak Pidana Siber Badan Reserse Kriminal Kepolisian Republik Indonesia (Bareskrim Polri) telah membentuk sebuah tim dalam penyelidikan kasus ini. Upaya lain juga dilakukan oleh kementria Komunikasi dan Informatika (kemenkominfo) serta Direktorat Jenderal Kependudukan dan Pencatatan Sipil (Ditjen Dukcapil). Dengan adanya kasus kebocoran data BPJS menandakan bahwa keamanan data di sektor ini masih belum siap.

Kasus kebocoran tersebut tentunya melanggar prinsip *Data Security, Data Privacy dan Ethics*, Data Security atau keamanan data merupakan mekanisme yang melindungi sekumpulan database terhadap berbagai ancaman yang sengaja atau tidak sengaja terjadi. Adanya motif pencurian data menyebabkan hilangnya kerahasiaan, privasi, ketersediaan dan integritas dari BPJS Kesehatan. Kebocoran data tersebut tentunya mengakibatkan kerugian secara materil atau pun non-materil

terhadap keberlangsungan pelayanan kesehatan di Indonesia. Hal tersebut juga menyebabkan hilangnya kredibilitas atau kepercayaan masyarakat Indonesia terhadap pemerintah.

Ditinjau dari prinsip *ethics* atau etika, peraturan terbaru mengenai pengelolaan data kesehatan, yakni *The health Insurance portability and Accountability Act* telah diterbitkan. Di dalamnya telah diatur mengenai privasi informasi pasien, standar keamanan data pasien serta transaksi yang terjadi dan lain-lain. Tentunya kebocoran data kesehatan tersebut mengakibatkan hilangnya privasi pengguna BPJS bahkan dapat digunakan untuk *cybercrime* seperti pemalsuan data, pemerasan, penipuan, hingga praktik *doxing*. Prosedur pendaftaran BPJS yang terlalu berbelit belit dan berbeda beda kondisi di setiap wilayah juga menjadi salah satu permasalahan yang memungkinkan potensi kebocoran data terjadi, Selain itu, minimnya pengetahuan mengenai keamanan data dari masyarakat Indonesia juga mengakibatkan mudahnya transaksi data diri dari satu orang ke orang yang lainnya.

Salah satu upaya terbesar yang dilakukan pemerintah untuk mencegah keamanan data saat ini ialah mempererat kerja sama dengan Badan Siber dan Sandi Negara (BSSN), bahkan Kepala Badan Siber dan Sandi Negara (BSSN) Hinsa Siburian menandatangani nota kesepahaman bilateral baru bersama Duta Besar Amerika Serikat pada 4 Desember 2024 untuk memperkuat kerja sama di bidang siber.

Amerika Serikat menyediakan bantuan keamanan siber sekitar Rp.63,4 miliar kepada Indonesia sejak tahun 2022 dan telah bekerja sama erat dengan BSSN selama dua tahun terakhir ini melalui pelatihan keamanan siber yang difokuskan pada penanggulangan ancaman bersama, pengembangan kemitraan dengan industri AS, dan pengembangan proyek keamanan siber. Ancaman siber di Indonesia akan terus ada seiring dengan meningkatnya penggunaan teknlogi digital di berbagai sektor. Ancaman ini sangat amat berdampak besar bagi individu, organisasi, dan pemerintah.

V. KESIMPULAN

Keamanan data dan pencegahan kebocoran data adalah masalah yang sangat penting baik di sektor publik maupun swasta. Meskipun sektor swasta memiliki lebih banyak sumber daya untuk menangani isu ini, kedua sektor tersebut tetap dihadapkan pada tantangan yang serupa, seperti ancaman siber yang terus berkembang dan pentingnya melindungi informasi pribadi. Dengan penerapan kebijakan yang tepat, peningkatan kesadaran, serta penggunaan teknologi keamanan yang efektif, baik sektor publik maupun swasta dapat mengurangi risiko kebocoran data dan melindungi informasi sensitif dari ancaman yang merugikan. Maka dari itu tingkat pengetahuan mengenai keamanan data di lingkup masyarakat juga sangat penting untuk dilakukan. Karena, hal tersebut merupakan *filter* atau langkah pertama kali dimana data dari setiap individu diperguunakan oleh pihak yang belum tentu dapat menjadi privasi dan keamanan dari data yang dimiliki,

VI. REFERENSI

Tjandrawinata, Raymond., (2016). Industri 4.0: Revolusi Abad Ini Dan Pengaruhnya Pada Bidang Kesehatan Dan Bioteknologi.

Waseso, R, (2022) BPJS Kesehatan Proyeksikan Jumlah Peserta di 2022 Capai 88,51% dari Populasi. https://keuangan.kontan.co.id/news/bpjs-kesehatan-proyeksikan-jumlahpeserta-di-2022-capai8851-dari-populasi

Oktaviani, S., Dewata, Y. J., & Fadlian, A., (2021). PERTANGGUNG JAWABAN PIDANA KEBOCORAN DATA BPJS DALAM PERSPEKTIF UU ITE.

Putra, C. A., & Masnun, M. A., ANALISIS PERTANGGUNGJAWABAN RUMAH SAKIT TERKAIT

Fajar Nugraha. (2024, December 5). Hadapi Ancaman, Indonesia-AS Sepakati Kerja Sama Keamanan Siber. https://www.metrotvnews.com/read/KdZCW5Jj-hadapi-ancaman-indonesia-as-sepakati-kerja-sama-keamanan-siber

Elfira Rahma, P. (2022, Juni 12). Analisis Kasus Kebocoran Data BPJS dalam Perspektif Data Security, Privacy, dan Ethics. https://www.kompasiana.com/elfirarahmaputri9964/62a58a52fdcdb4707c2c7ef7/analisis-kasus-kebocoran-data-bpjs-dalam-perspektif-data-security-privacy-dan-ethics