KEBOCORAN DATA MEDIS KEMENKES, DATA PENGGUNA APLIKASI KREDIT DIGITAL, DAN DATA PELAMAR KERJA PT PERTAMINA *TRAINING* & *CONSULTING* DI NEGARA *OPEN SOURCE* UNTUK DIPERJUALBELIKAN

Faishal Akbar Syahputra

Universitas Muhammadiyah Malang, Jalan Raya Tlogomas No. 246 Malang 65141
Surel: faishalas39@webmail.umm.ac.id

ABSTRAK: Artikel ini membahas tentang Kebocoran Data Medis Kemenkes, data Pengguna Aplikasi Kredit Digital, dan Data Pelamar Kerja PT Pertamina *Training* & *Consulting* di Negara *Open Source* untuk Diperjualbelikan. Data adalah sekumpulan informasi atau bisa juga sebagai keterangan dari berbagai hal yang berasal dari pengamatan atau pencarian ke berbagai sumber. Kebocoran data atau *Data Leakage* adalah kondisi dimana terjadi transmisi data sensitif yang tidak sah atau sebuah kondisi dimana data bisa diakses oleh pihak yang tidak berwenang kemudian disebarluaskan untuk diperjualbelikan dalam sebuah forum. Kebocoran data ini dapat terjadi karena kelalaian dari pengguna itu sendiri saat sedang berselancar di internet ataupun karena sistem keamanan suatu website tersebut yang sangat rendah, sehingga rentan dibobol oleh seseorang yang memiliki keahlian khusus dalam dunia internet. Kebocoran data ini terjadi karena semakin berkembangnya zaman sehingga semua proses verifikasi data dilakukan secara *online*, namun tidak diikuti dengan kemajuan SDM dan peningkatan keamanan suatu website sehingga dapat terjadi kebocoran data. Kebocoran data ini biasanya terjadi melalui *link phising*, *e-mail*, aplikasi yang bergerak pada bidang *finance* dan *e-commerce*, dan pada website resmi suatu instansi. Kebocoran data ini lebih sering terjadi dalam website resmi instansi pemerintahan yang berisi data sensitif, maka dari itu Indonesia mendapat julukan sebagai "Negara *open source*" karena sering terjadi kebobolan dalam website resmi tersebut. Data sensitif yang biasanya tersebar dan diperjualbelikan dalam suatu forum adalah data pribadi seseorang seperti nama lengkap, nama ibu kandung, tanggal lahir, alamat, *e-mail*, *password*, nomor telepon, dan hal-hal penting lainnya. Data-data yang bocor kemudian diperjualbelikan ini rentan disalahgunakan oleh oknum yang tidak bertanggung jawab. Apabila data yang disalahgunakan tersebut adalah KTP seseorang, maka bisa digunakan sebagai sarana penipuan dalam jual beli, atau bahkan digunakan dalam pengajuan data aplikasi *finance* seperti pinjaman *online*. Penyalahgunaan data yang diperjualbelikan dalam bidang *finance* atau pinjaman *online* biasa disebut sebagai *cybercrime economy*.

Kata Kunci: data medis kemenkes, data pengguna aplikasi kredit digital, data pelamar kerja, diperjualbelikan, kebocoran data, negara *open source*.

Data pribadi atau identitas seseorang merupakan hal yang sangat privasi dan harus terjaga. Semakin berkembangnya zaman, teknologi semakin berkembang dan hampir mempermudah segala urusan sehingga semuanya bisa dilakukan dari rumah. Karena zaman dan teknologi semakin berkembang, hampir semua data-data yang kita gunakan untuk

melengkapi berkas disimpan dalam suatu *database*. Hal ini sangat mempermudah urusan jika data tersebut dibutuhkan. Sudah banyak data kita yang tersimpan dalam *database* suatu instansi atau perusahaan, contohnya adalah data medis, data verifikasi bank, identitas pribadi untuk keperluan sekolah, kuliah, ataupun pekerjaan, dan masih banyak lagi. Dengan berkembangnya zaman dan teknologi ini, diharapkan diikuti dengan peningkatan keamanan *database* dan *skill* dari pengelola *database* tersebut, mengingat data yang tersimpan merupakan data yang sensitif dan dapat disalahgunakan apabila tersebarluas.

Namun sayangnya, pada tahun 2021, terjadi lebih dari 10 (sepuluh) kali kasus kebocoran data di Indonesia. Yang mana sebagian besar data tersebut bocor dari *database* resmi pemerintahan Indonesia. Data-data yang berhasil diretas adalah sertifikat vaksin presiden, *database* Polri, *database* KPAI (Komisi Perlindungan Anak Indonesia), *database* BPJS, dan data pengguna aplikasi Facebook. Kebocoran data yang terjadi pada pengguna Facebook ini terjadi pada April 2021, sekitar 130.000 data pengguna menjadi korban kebocoran data ini. Data tersebut berisi nama lengkap pengguna, tanggal lahir, *email*, jenis kelamin, dan *password*. Sekitar satu bulan setelah kejadian tersebut, kebocoran data kembali terjadi pada *database* BPJS Kesehatan. Isi dari data yang bocor dari BPJS hampir sama dengan bocornya data facebook, yaitu nama lengkap, email, nomor *handphone*, jenis kelamin, nomor induk kependudukan (NIK), dan juga alamat. Selanjutnya pada Agustus, terjadi kebocoran data pada aplikasi buatan pemerintah, yaitu eHAC. Data ini berisi informasi yang berkaitan dengan riwayat kesehatan, perjalanan, dan data pribadi pengguna seperti hasil tes *covid*, *email*, serta nomor *handphone* dan *passport*. Selain itu, juga terjadi kebocoran data pada berbagai aplikasi yang berjalan pada sektor perbankan, perhotelan, dan di awal tahun terjadi kebocoran *database breach* imigrasi, *database breach* studybox.id, isi email pegawai bank BNI, *data breach* yang diduga dari binus.ac.id, data medis yang diklaim dari database kemenkes, data pengguna aplikasi pinjaman *online*, dan data pelamar kerja PT Pertamina *Training* & *Consulting*.

Berdasarkan dari kejadian kebocoran data yang sudah-sudah, data yang bocor ini kemudian dijual oleh seseorang yang berhasil menjebol *database* itu. Data tersebut dijual dalam *darkweb* atau sebuah forum yang bernama raidforum. Raidforum adalah forum berbasis web yang tidak semua orang bisa bebas mengakses situs web tersebut. Harga yang dicantumkan tiap kasus kebocoran data berbeda-beda tergantung penjual data tersebut. Harga bisa mahal dan bisa juga murah karena tidak ada patokan resmi untuk memberi harga data tersebut. Sebagai contoh, data BPJS Kesehatan yang bocor pada Mei 2021 dijual dengan harga yang sangat tinggi yaitu 84.000.000 (84 juta) sedangkan data aplikasi eHAC dijual dengan harga yang bisa dibilang murah yaitu 35.000 (35 ribu) per-data. Dengan maeaknya kebocoran

data yang terjadi pada 2021, maka skill pengelola *database* dari tiap instansi ataupun vendor aplikasi dapat ditingkatkan lagi dengan cara terus belajar, terus membaca, sharing dengan yang lainnya, mengikuti kursus, ataupun mengasah *softskill* yang dimiliki guna meminimalisir kebocoran data pada tahun 2022 dan seterusnya. Sehingga bisa meningkatkan keamanan dari sebuah *database* yang dikelola. Apabila terdapat indikasi *database* akan diretas, maka pengelola *database* dapat mencegah hal tersebut, dan kalaupun *database* tetap berhasil diretas, setidaknya pengelola dapat mencegah supaya data tersebut tidak sampai terjual dalam situs raidforum. Karena apabila seorang pengelola *database* tersebut tidak melakukan *upgrade* diri atau bahkan tidak kompeten dalam bidangnya, maka akan berdampak buruk bagi pemilik data yang tersimpan dalam *database* mereka karena ketika data tersebut diretas dan dijual, dapat disalahgunakan oleh oknum tertentu.

KEBOCORAN DATA MEDIS KEMENKES

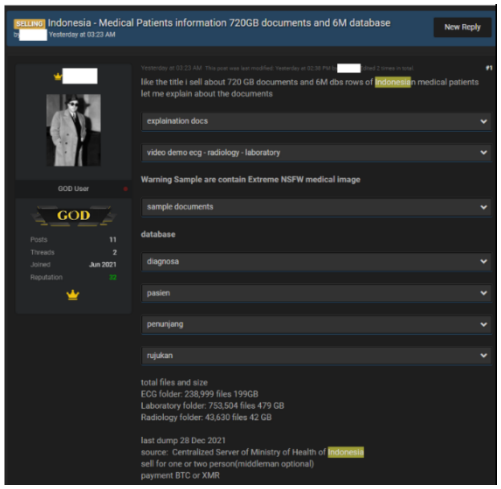
Kementrian Kesehatan Republik Indonesia (Kemenkes RI), adalah kementrian dalam pemerintahan yang bergerak dalam bidang kesehatan. Kemenkes ini didirikan pada 19 Agustus 1945. Kemenkes memiliki tugas membantu Presiden untuk menyelesaikan sebagian urusan pemerintahan dalam bidang kesehatan. Fungsi kemenkes ini sudah diatur dalam Permenkes 64 Tahun 2016, diantaranya adalah (1) pelaksanaan penelitian dan pengembangan di bidang kesehatan, (2) perumusan, penetapan, dan pelaksanaan kebijakan di bidang kesehatan masyarakat, (3) pencegahan dan pengendalian penyakit, (4) pelayanan kesehatan dan alat kesehatan, (5) dan pelaksanaan pengembangan dan pemberdayaan sumber daya manusia di bidang kesehatan serta pengelolaan tenaga kesehatan.

Karena kemenkes merupakan kementrian yang bergerak dalam bidang kesehatan, maka riwayat kesehatan setiap orang tersimpan pada *database* kemenkes. Data tersebut berasal dari berbagai rumah sakit dan perusahaan kesehatan yang berada di Indonesia. Data tersebut biasanya berisi nama lengkap, tempat tanggal lahir, jenis kelamin, riwayat penyakit, dan lainnya yang berkaitan dengan identitas diri dan kesehatan. Sudah seharusnya data tersebut dirahasiakan dan disimpan dalam *database* yang aman. Namun sayangnya, pada 28 Desember 2021 ada seseorang yang berhasil meng-*dump* data yang diklaim dari *database* kemenkes itu pada situs raidforum. Data yang berhasil di*dump* pada situs raidforum itu berisi informasi sensitif pasien sebesar 3 GB dengan 3 folder yang berisi 4.763 *files* yang berupa dokumen, gambar, dan video. Sedangkan ukuran asli *file* yang diklaim berhasil diretas oleh seseorang tersebut adalah sebanyak 720 GB dokumen dan 6 Juta *database*. Diantaranya adalah ECG Folder yang berisi 238.999 *files* sebesar 199 GB, *laboratory* folder yang berisi 753.504 *files*

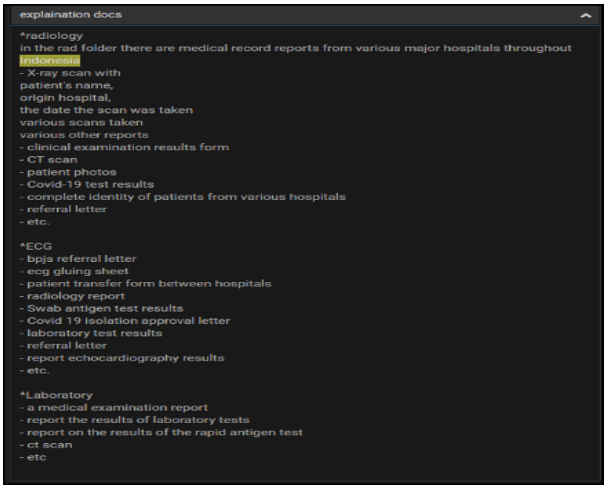
sebesar 479 GB, dan *radiology* folder yang berisi 43.630 *files* sebesar 42 GB. ECG *lab* adalah tes diagnostik yang digunakan untuk mengetahui kondisi jantung yang diambil dengan cara memasang *electrode* pada badan. Sedangkan *radiology scan* biasanya berisi gambar jaringan lunak, tulang, dan pembuluh darah pasien. Sedangkan *database* yang berhasil di*dump* adalah *database* diagnosa, pasien, penunjang, dan rujukan.

Pada *database* diagnosa, format *database* tersebut adalah (id_rujukan, anamnesis, icd10, kriteria_rujukan, diagnosa, kesadaran, gcs, tensi, nadi, suhu, pernapasan, nyeri, kondisi_umum, status). Format tersebut merupakan format dari seorang pasien ketika di diagnosa di rumah sakit. Untuk *database* pasien, format yang tersebar adalah (nama, no_kontak, alamat, tempat_lahir, tgl_lahir, jenis_kelamin, no_kartu_jkn, nik). Sedangkan untuk *database* rujukan, format yang tersebar adalah (id_rujuk, no_rujukan_bpjs, transportasi, alasan_merujuk, tgl_rujuk, nik_petugas, nama_petugas). Pada folder ECG yang berisi 238.999 *files*, diantaranya adalah (1) surat rujukan BPJS, (2) lembar ECG, (3) transfer pasien dari berbagai rumah sakit, (4) laporan *radiology*, (5) hasil tes *swab antigen*, (6) surat persetujuan isolasi covid-19, (7) hasil tes laboratorium, (8) surat rujukan, (9) laporan hasil ECG, (10) dan lain-lain. Untuk folder *laboratory* yang berisi 753.504 *files*, diantaranya berisi (1) laporan pemeriksaan medis, (2) laporan hasil tes laboratorium, (3) laporan hasil tes antigen, (4) CT *scan*, (5) dan lain-lain. Sedangkan pada folder *radiology* yang berisi 43.630 *files*, isinya adalah (1) *x-ray scan* dengan nama pasien, rumah sakit asal, tanggal *scan*, *various scans taken*, dan *various other reports*. (2) hasil pemeriksaan klinis, (3) CT *scan*, (4) foto dan video pasien, (5) hasil tes covid-19, (6) identitas lengkap pasien dari berbagai rumah sakit, (7) surat rujukan, (8) dan lain-lain.

Semua data yang dijabarkan diatas adalah data *sample* dari seorang yang berhasil meretas *database* kemenkes yang ditampilkan pada situs raidforum untuk dijual. Data tersebut dijual per satu atau dua orang, dengan sistem pembayaran menggunakan mata uang BTC atau XMR. Data yang bocor tersebut diklaim dari kemenkes karena pada data tersebut berisi dokumen dengan berbagai kop surat dari rumah sakit yang berada di Indonesia, yang mana kemenkes merupakan “pusat” dari para rumah sakit tersebut. Selain yang sudah disebutkan diatas, data pribadi pasien seperti nama lengkap, nomor telepon, alamat, tempat tanggal lahir, jenis kelamin, nomor kartu Jaminan Kesehatan Nasional (JKN), Nomor Induk kependudukan (NIK), foto Kartu Tanda Penduduk (KTP), dan Kartu Indonesia Sehat (KIS). Pada raidforum tersebut, tidak hanya data kemenkes saja yang dijual, namun ada berbagai data pribadi lainnya seperti data pengguna aplikasi kredit digital.

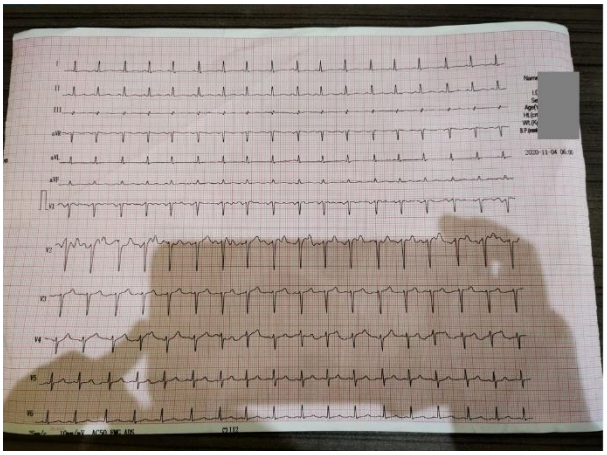


Gambar 1 - Kiriman di Raidforum



Gambar 2 – Isi dari Setiap Folder

Gambar 3 – Kop Surat dari Berbagai Rumah Sakit

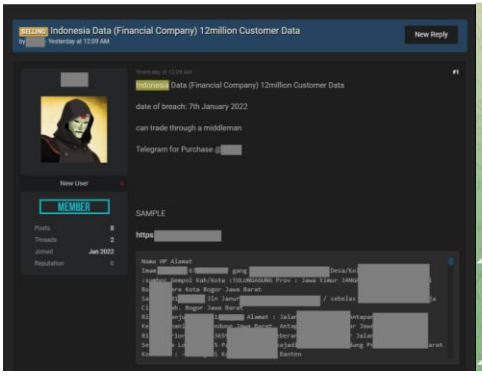


Gambar 4 – Sample ECG

KEBOCORAN DATA PENGGUNA APLIKASI KREDIT DIGITAL

Semakin berkembangnya zaman dan teknologi, ketika sedang memerlukan uang, tidak perlu lagi bersusah payah meminjam kepada rentenir ataupun tetangga dengan syarat yang rumit dan bunga yang besar. Sekarang sudah banyak aplikasi untuk mengajukan pinjaman uang ataupun kredit barang dengan syarat hanya dengan foto KTP dan foto *selfie* memegang KTP pribadi. Kelebihan dari aplikasi seperti ini adalah tingkat bunga yang rendah, proses cepat dan gampang, jaminan yang tidak rumit dan aman karena terdaftar dalam Otoritas Jasa Keuangan (OJK). Aplikasi kredit yang terdaftar dalam OJK adalah (1) Danamas, (2) Investree, (3) Amartha, (4) Maucash, dan (5) Finmas. Namun ada juga beberapa aplikasi kredit digital yang rawan digunakan karena belum terdaftar dalam OJK seperti (1) TunaiSaku, (2) Dana Impian, (3) Kredit Kilat, dan (4) Akulaku. Bahaya dari aplikasi illegal seperti ini adalah (1) biaya dan denda jatuh tempo tidak transparan dan sangat besar, (2) tidak ada regulator khusus yang mengawasi kegiatan dalam aplikasi, (3) cara penagihan yang kasar, tidak manusiawi, dan bertentangan hukum, (4) lokasi kantor yang tidak jelas untuk menghindari aparat hukum, dan (5) keamanan data dalam aplikasi kurang terjamin keamanannya.

Pada 7 Januari 2022, sebanyak 12 juta data pengguna aplikasi kredit digital akulaku bocor. Kemudia data tersebut dimasukkan kedalam situs raidforum pada tanggal 13 Januari pukul 00.09. pada situs tersebut dituliskan “Indonesia Data (Financial Company) 12 Million Customer Data”. Disitu juga terlampir tanggal *data breach*, informasi akun telegram penjual untuk pembelian data yang dijual, serta diberikan *sample* kebocoran data tersebut. Seseorang mencoba menghubungi penjual tersebut untuk menanyakan darimana asal data tersebut, kemudian sang penjual menjawab bahwa data tersebut berasal dari perusahaan akulaku. Sedangkan untuk *sample* data yang diberikan, kurang lebih berisi 30 data. Data-data tersebut berisi nama pengguna lengkap dengan nomor telepon dan alamat rumah. Sebagai contoh adalah sebagai berikut : “Imam – 670xxxxxxxx – Gang xx, Desa/Kelurahan xx, Sumber Gempol Kab/Kota Tulungagung, Provinsi Jawa Timur” dan “Salaxx – 628xxxxxxxxxx – Jl. Janurxx, sebelas, Cixx, Kab. Bogor Jawa Barat”. Beberapa hari sebelum kebocoran data ini, tepat pada tanggal 8 Januari, juga terjadi kebocoran data pelamar kerja di PT Pertamina *Training* & *Consulting*.



Gambar 5 - Kiriman di Raidforum

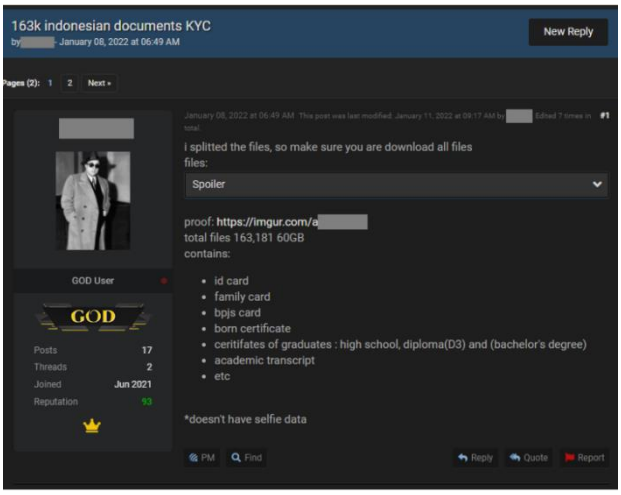
Gambar 6 – Chat Telegram dengan Penjual

KEBOCORAN DATA PELAMAR KERJA PT PERTAMINA *TRAINING* & *CONSULTING*

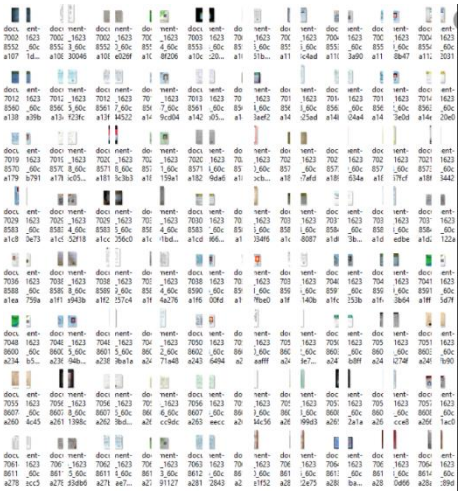
Pada Desember dan Januari 2021, PT Pertamina *Training* & *Consulting* kembali membuka lowongan pekerjaan untuk usia 18-45 tahun dengan lulusan SMA, SMK, D1, D3,S1 dan S2 dengan posisi *Accounting*, manager, ahli komputer, IT, statistika, supervisor, laboratorium, staf lapangan, sekuriti, dan masih banyak lagi. Dengan kriteria memiliki kemampuan dalam bidang, analisa yang baik, komunikasi yang baik, teliti, disiplin, dapat bekerja dalam tim, bertanggung jawab, dan memiliki motivasi kerja yang tinggi. Pelamar kerja akan mendapat fasilitas (1) Jamsostek, (2) bonus bulanan, (3) penghasilan 10 – 20 juta/bulan, dan (4) uang makan & *transport* 75 ribu/hari. Pelamar akan ditempatkan di Indonesia atau sesuai dengan domisili terdekat. Kelengkapan berkas yang harus dimiliki pelamar kerja adalah

(1) surat lamaran dan daftar riwayat hidup, (2) fotokopi ijazah dan transkrip nilai, (3) fotokopi KTP dan pas foto 4x6, dan (4) nomor telepon dan *email* yang valid.

Namun, pada 8 Januari pukul 06.49 pagi, data-data para pelamar tersebut ditemukan dalam situs raidforum. Total data yang dibagikan kedalam forum tersebut sebanya 163.181 *files* dengan ukuran total sebanyak 60 GB. Dalam situs tersebut, penulis melampirkan bahwa data yang tertera berisi (1) KTP dan SIM, (2) kartu keluarga dan kartu BPJS, (3) akte kelahiran, (4) ijazah SMA, D3 dan Sarjana, (5) transkrip nilai, (6) NPWP dan tidak terdapat foto *selfie* dengan KTP. Dengan bocornya data pelamar ini ditakutkan data disalahgunakan untuk mengaktifkan nomor perdana, pendaftaran akun, penipuan, dan masih banyak lagi. Berbeda dengan dua data yang telah dibahas sebelumnya, yang mana dua data sebelumnya itu diperjualbelikan, namun data pelamar kerja ini hanya di-*dump* secara cuma-cuma dan tidak diperjualbelikan. Kominfo telah buka suara mengenai hal ini, juru bicara kominfo, Dedy Permadi mengatakan bahwa "Kementrian Komunikasi dan Informatika sedang menindaklanjuti dan menelusuri dugaan kebocoran data pelamar kerja pada PT Pertamina Training & Consulting (PTC), diantaranya dengan meminta informasi secara formal dari jajaran Direksi PTC guna mendapatkan klarifikasi lebih lanjut". Selain itu pihak kominfo juga meminta setiap Penyelenggara Sistem Elektronik (PSE) wajib memberitahukan secara tertulis kepada Pemilik Data Pribadi (PDP) apabila gagal melindungi kerahasiaan data pribadi dalam sistem yang mereka kelola.



Gambar 7 - Kiriman di Raidforum



Gambar 8 – Foto KTP & SIM

Gambar 9 – Foto Kartu Keluarga

Gambar 10 – Foto Ijazah

PENUTUP

Simpulan

Tingkat keamanan *database* dan *skill* pengelola *database* di Indonesia masih sangat lemah, sehingga masih sering terjadi kebocoran data yang kemudian diperjualbelikan atau bahkan di-*dump* begitu saja pada sebuah situs internet. Situs tersebut adalah raidforum, yang mana merupakan situs yang berisi penjualan atau bahkan pembuangan data-data dari *database* yang berhasil diretas oleh seseorang. Penjualan data tersebut bisa dilakukan menggunakan mata uang BTC atau XMR. Kebocoran dan penjualan data dapat berdampak negatif bagi pemilik data karena dapat disalahgunakan untuk kejahatan tertentu seperti penipuan, melakukan aktivasi akun, dan masih banyak lagi.

Saran

Dengan adanya tulisan ini, diharapkan kepada pengelola sistem *database* untuk lebih meningkatkan keamanannya kembali, dan meningkatkan *skill* dari pengelola itu sendiri supaya kedepannya semakin sedikit bahkan tidak lagi terjadi kebocoran data yang kemudian diperjualbelikan atau hanya di bagikan secara cuma-cuma pada sebuah forum, karena dapat berdampak buruk bagi pemilik data tersebut.

DAFTAR RUJUKAN

Acer Indonesia. (2021). *Kebocoran Data (Data Leakage), Kenali Penyebabnya dan Dampaknya*. Diakses pada 14 Januari 2022, dari https://commercial.acerid.com/support/articles/kebocoran-data-data-leakage-kenali-penyebab-dan-dampaknya

E-Commerce Shitposting V 2.0. (2022). *Data Pelamar Kerja di PT Pertamina Training & Consulting*. Diakses pada 18 Januari 2022, dari https://www.facebook.com/ecommerceshitpostingv2/posts/154884700216813

E-Commerce Shitposting V 2.0. (2022). *Kebocoran Data dari Salah Satu Perusahaan Finance di Indonesia*. Diakses pada 18 Januari 2022, dari https://www.facebook.com/ecommerceshitpostingv2/posts/154741760231107

E-Commerce Shitposting V 2.0. (2022). *Kebocoran Data Lain Sebagai Informasi yang Mungkin Berhubungan dengan Anda.* Diakses pada 15 Januari 2022, dari https://www.facebook.com/ecommerceshitpostingv2/posts/154887060216577

E-Commerce Shitposting V 2.0. (2022). *Lebih Detail Soal Kebocoran Data Medis di Kemenkes.* Diakses pada 17 Januari 2022, dari https://www.facebook.com/ecommerceshitpostingv2/posts/153225253716091

E-Commerce Shitposting V 2.0. (2022). *Telah Terjadi Breach Data yang Diklaim dari Database Kemenkes.* Diakses pada 17 Januari 2022, dari https://www.facebook.com/ecommerceshitpostingv2/posts/153084467063503

Jemadu, L, dkk. (2021). *Daftar Kasus Kebocoran Data di Indonesia Selama 2021, Termasuk Sertifikat Vaksin Jokowi.* Diakses pada 16 Januari 2022, dari https://www.suara.com/tekno/2022/01/01/015822/daftar-kasus-kebocoran-data-di-indonesia-selama-2021-termasuk-sertifikat-vaksin-jokowi?page=1

Kementrian Kesehatan Republik Indonesia. (2021). *Tugas dan Fungsi*. Diakses pada 17 Januari 2022, dari http://p2p.kemkes.go.id/tugas-dan-fungsi/

NKD, Feradhita. (2020). *Mengenal Apa yang Dimaksud dengan Kebocoran Data (Data Leakage)?*. Diakses pada 15 Januari 2022, dari https://www.logique.co.id/blog/2020/10/22/kebocoran-data/

Otoritas Jasa Keuangan. *Bahaya Fintech P2PL Ilegal*. Diakses pada 18 Januari 2022, dari https://www.ojk.go.id/id/kanal/iknb/data-dan-statistik/direktori/fintech/Documents/P2PL%20legal%20vs%20ilegal.pdf

Satria, Rio A, dkk. (2021). *Pengantar Data*. Diakses pada 14 Januari 2022, dari https://wageindicator-data-academy.org/countries/data-akademi-garmen-indonesia-bahasa/teknis-menganalisa-data-hasil-survei/pengertian-data

Sehertian, F. (2022). *Kominfo Buka Suara Soal Dugaan 160 Ribu Pelamar Pertamina Dijual Hacker*. Diakses pada 18 Januari 2022, dari https://kumparan.com/kumparantech/kominfo-buka-suara-soal-dugaan-160-ribu-pelamar-pertamina-dijual-hacker-1xIYIqyYGAU/full?fbclid=IwAR1hTHfKocoXltOFbWT1pksmkzoIa5X6Y8RIvFM4rtAoKPNBauvcooS-FGQ

Wibowo, Patrick Trusto J. (2021). *Apa Itu Data Leakage.* Diakses pada 14 Januari 2022, dari https://wartaekonomi.co.id/read364194/apa-itu-data-leakage