Jurnal Hukum Progresif

Vol 7 No 1, Jan 2024
EISSN : 24490120

ANALISA KASUS KEBOCORAN DATA PENGGUNA TOKOPEDIA

Qodri Bestari[1], **Degita Armelia Putri**[2], **Kireina Ajeng Kurnia**[3]
qbestari8@gmail.com[1] , degitadegitaarmeliaputri@gmail.com[2], kireinaajeng123@gmail.com[3]
Universitas Pakuan

Abstrak: Keamanan data dan perlindungan privasi pengguna telah menjadi isu penting di era digital, terutama mengingat pesatnya pertumbuhan bisnis online. Pelanggaran data Tokopedia pada tahun 2020 adalah salah satu insiden yang menyoroti masalah serius dalam keamanan data dan perlindungan privasi konsumen. Penelitian ini menjelaskan lebih lanjut sejarah pembobolan data Tokopedia, implikasinya dalam konteks keamanan data dan perlindungan konsumen, serta tindakan yang diambil oleh otoritas dan perusahaan dalam menanggapi kejadian ini. Penelitian ini bertujuan untuk memberikan wawasan lebih dalam mengenai isu - isu penting keamanan data dan perlindungan data dalam bisnis online dengan meninjau latar belakang dan hasil dari kejadian ini.
Kata Kunci: Keamanan Data, Bisnis Online, Perlindungan Konsumen.

PENDAHULUAN

Cybercrime adalah kejahatan yang melibatkan perangkat komputer atau jaringan. Kejahatan ini biasanya dilakukan secara online. Fakta nya, kejahatan dunia maya ini bisa menyerang biasa saja. Jika anda menjadi salah satu korbannya, pasti akan menimbulkan kerugian yang besar ini memengaruhi kondisi mental anda dan bahkan kerugian finansial.

Contoh kejahatan dunia maya yang sangat berbahaya mencakup penindasan maya, pencurian identitas, dan kebocoran informasi pribadi yang mengarah pada penyebaran informasi pribadi yang mengarah pada penyebaran informasi pribadi melalui internet. Tujuan kampanye ini sangat beragam. Memanfaatkan orang lain, mulai dari ancaman, intimidasi, hingga penghinaan. Dengan pesatnya kemajuan teknologi dan internet, ancaman kejahatan dunia maya semakin meningkat. Tentu saja, untuk melindungi diri dari berbagai serangan siber, anda perlu mengetahui cara mencegahnya.
Berikut ini cara mencegah kejahatan dunia maya :

a. Jangan gunakan perangkat lunak bajakan. Aplikasi dan perangkat lunak bajakan rentan terhadap virus malware, sehingga menggunakan perangkat lunak bajakan membuat data anda beresiko dicuri atau rusak
b. Jangan mudah percaya dan selalu waspada. Jangan mudah percaya pada seseorang yang baru ditemui. Saat menggunakan internet, anda harus selalu berhati - hati karena banyak bahaya yang dipertaruhkan. Selain itu, jangan hanya mencari situs informasi di internet, apalagi website.
c. Jangan membagikan informasi pribadi dan tidak mengunggah informasi pribadi atau apa pun yang berhubungan dengan informasi pribadi ke media sosial.
d. Jangan gunakan kata sandi yang sama untuk semua akun anda. Hal ini dapat dengan mudah ditebak oleh penjahat yang mengincar akun media sosial anda, akun lain, bahkan mengambil alih mbanking anda.

Keamanan data dan perlindungan privasi pengguna telah menjadi isu penting di era digital, terutama mengingat pesatnya pertumbuhan bisnis online. Pelanggaran data Tokopedia pada tahun 2020 adalah salah satu insiden yang menyoroti masalah serius dalam keamanan data dan perlindungan privasi konsumen. Investigasi ini menyelidiki latar belakang insiden pembobolan data pengguna Tokopedia dan menyajikan berbagai aspek terkait insiden tersebut. Latar belakang penelitian ini mencakup beberapa poin penting:

a) Pentingnya data pribadi dalam bisnis online: Dalam ekosistem bisnis online yang berkembang pesat, data pribadi pengguna sangat berharga. Penulis mengumpulkan dan memelihara data ini untuk berbagai tujuan, termasuk personalisasi layanan, pemasaran, dan analitik.
b) Pertumbuhan e-commerce di Indonesia: Industri e-commerce telah berkembang secara signifikan di Indonesia, dengan platform seperti Tokopedia menjadi pemain utama di pasar ini. Dengan pertumbuhan ini, perusahaan mengumpulkan data dalam jumlah besar dari penggunanya.
c) Insiden pelanggaran data Tokopedia : Pada bulan Juni 2020, laporan pelanggaran data pengguna Tokopedia mengejutkan publik. Jutaan informasi pribadi pengguna, termasuk nama, alamat email, nomor telepon, dan alamat surat, disebarkan di forum gelap di Internet.
d) Reaksi masyarakat dan pihak berwenang : Kejadian ini menimbulkan kekhawatiran besar masyarakat. Pihak berwenang di Indonesia, termasuk Kementerian Komunikasi dan Informatika dan Komisi Perlindungan Data Pribadi (KPDP), terlibat dalam penyelidikan tersebut dan menekankan pentingnya perlindungan data dan privasi pengguna.
e) Implikasi Keamanan Data : Kasus ini menyoroti tantangan keamanan data yang dihadapi organisasi dalam menghadapi ancaman kejahatan dunia maya. Perusahaan online harus menjaga integritas data pengguna untuk membangun kepercayaan dan mematuhi peraturan privasi yang semakin ketat.
f) Perlindungan Konsumen dan Hak Perlindungan Data: Kasus ini menggambarkan pentingnya hak perlindungan konsumen dan perlindungan data. Pengguna bisnis online berhak atas informasi yang benar, privasi yang dihormati, dan perlindungan data yang ketat.

Penelitian ini menjelaskan lebih lanjut sejarah pembobolan data Tokopedia, implikasinya dalam konteks keamanan data dan perlindungan konsumen, serta tindakan yang diambil oleh otoritas dan perusahaan dalam menanggapi kejadian ini. Penelitian ini bertujuan untuk memberikan wawasan lebih dalam mengenai isu - isu penting keamanan data dan perlindungan data dalam bisnis online dengan meninjau latar belakang dan hasil dari kejadian ini.

METODE PENELITIAN

Metode penelitian yang penulis gunakan adalah metode normatif, yaitu pendekatan yang dilakukan melalui kajian terhadap pokok bahasan hukum dengan mengkaji seluruh asas hukum yang berpedoman pada konsep, teori dan hukum. Hal ini merupakan bagian dari keterkaitan norma - norma yang terdapat dalam Undang - Undang Dasar Negara Republik Indonesia. Untuk melengkapi penelitian penelitian ini, penulis juga menggunakan metode observasi. Ini adalah metode fasilitasi lain yang melihat rangkaian peristiwa di masa lalu dan merangkum setiap situasi yang tampaknya penting untuk digunakan dalam pembelajaran di masa depan. Suatu penelitian dimana penulis melakukan penelitian dari segala sumber yang memberikan informasi kepada penulis.

PEMBAHASAN

Kronologi lengkap terjadinya kebocoran data pengguna tokopedia

Pertama, seorang hacker bernama Whysodank memberikan informasi detail sekitar 15 juta akun pengguna Tokopedia ke forum RaidForums. Karena algoritme kata sandi akun selalu di hash, peretas dapat berbagi data dan mencari bantuan dari peretas lain untuk membuka kunci algoritme kata sandi akun. Data yang diberikan meliputi ID pengguna, alamat email, nama, tanggal lahir, jenis kelamin, nomor ponsel, dan kata sandi terenkripsi. Ia mengklaim data tersebut berasal dari serangan hacker pada 20 Maret 2020. “Saya memutuskan untuk membagikan sebagian data dari data dump Tokopedia yang [diretas] mulai Maret 2020 dan saya akan membagikan 15 juta keping data lagi,” tulisnya di ReidForums., Senin (4 Mei 2020).

Keesokan harinya, peretas mengumumkan bahwa mereka menjual 91 juta data seharga 5.000 USD atau setara dengan Rp 75 juta. Dia menjualnya di Empire Market, pasar gelap di web gelap. Manajemen Tokopedia sendiri mengakui adanya upaya pencurian data pengguna Tokopedia, namun informasi sensitif seperti password tetap terlindungi. Razak, wakil presiden komunikasi di Tokopedia Corporate, mengatakan: “Meskipun kata sandi pengguna dan informasi sensitif dilindungi dengan enkripsi, kami terus mendorong pengguna Tokopedia untuk secara teratur mengubah kata sandi akun mereka untuk memastikan keamanan dan kenyamanan.” Nuraini menambahkan, Tokopedia telah menerapkan keamanan berlapis, termasuk OTP, yang hanya bisa di akses oleh pemegang akun secara real time.

Kami juga selalu menyarankan kepada seluruh pengguna untuk tidak membagikan kode OTP miliknya kepada siapa pun dengan alasan apapun. “Tokopedia menjamin tidak ada data pembayaran yang hilang. Razak mengatakan dalam siaran pers nya, Minggu (5 Maret): “Seluruh transaksi menggunakan metode pembayaran apa pun, termasuk kartu debit, kartu kredit, dan informasi OVO di Tokopedia, tetap aman”. Menanggapi pelanggaran data tersebut, perusahaan media dan IT Johnny Gerald Plate meminta direktur platform digital Tokopedia untuk melakukan penyelidikan internal. Tujuannya adalah untuk mengidentifikasi dugaan pelanggaran perlindungan data pada platform marketplace dan mengambil tindakan yang diperlukan untuk menjamin keamanan data pengguna. “Ditulis bekerja sama dengan Tokopedia.

Johnny mengatakan pada Minggu, 3 Mei 2020, tim teknis Kominfo melakukan penyesuaian teknis untuk memantau permasalahan pelanggaran data pengguna, mengutip siaran pers Kementerian Informasi dan Komunikasi Jakarta Media. Johnny mengatakan Kementerian Informasi dan Komunikasi meminta Tokopedia melakukan tiga hal untuk menjamin keamanan data pengguna. “Hal

pertama yang harus dilakukan Tokopedia adalah segera mengamankan sistem nya untuk mencegah pelanggaran data yang meluas. Kami kemudian akan memberi tahu pemegang akun yang informasi pribadinya mungkin telah di bobol. Dan ketiga, kami melakukan investigasi internal untuk memastikan dugaan pelanggaran data dan jika terjadi pelanggaran data, cari penyebabnya, jelasnya.

Sekretaris Jenderal NDP juga meminta laporan yang memberi tahu pemilik akun tentang dugaan pelanggaran data, langkah - langkah keamanan sistem yang diambil, dan kemungkinan dampak pelanggaran data terhadap data pemilik. “Kami masih menunggu laporannya selesai,” ujarnya. Tokopedia sebagai Penyelenggara Sistem Elektronik (PSE) harus mematuhi standar mengenai perlindungan data pribadi yang tertuang dalam Peraturan Pemerintah Nomor 71 Tahun 2019 dan Peraturan Kementerian Media dan Teknologi. “Tokopedia mengklaim sistem keamanannya menggunakan kata sandi yang disimpan dalam bentuk hash.

Selain itu, Tokopedia juga menggunakan fungsi OTP sebagai autentikasi dua faktor sehingga pengguna tidak bisa login. “Selalu minta pengguna untuk memasukkan kode baru secara real time setiap kali mereka memasukkan nya,” kata Johnny. Kementerian Informasi dan Komunikasi juga mengimbau masyarakat untuk menjaga keamanan akunnya. “Masyarakat harus sering-sering mengganti password dan jangan langsung percaya pada siapa pun yang meminta password atau kode OTP-nya. Jadi kalau ada yang minta password atau kode OTP, sudah pasti scam,” ujar Johnny. Sebelum mengeklik tautan yang diterima pengguna melalui email, harap verifikasi bahwa alamat email pengirim adalah asli.

“Beginilah cara pengguna membaca alamat dari belakang ke depan,” lanjutnya. Lebih lanjut Johnny menjelaskan Kementerian Informasi dan Komunikasi akan mengundang Direktur Tokopedia. Terkait hal itu, saya meminta Dirjen Aptics untuk mengadakan rapat direksi Tokopedia dan menjelaskan nya. Rencananya pertemuan akan dilakukan pada Senin, 4 Mei,” kata Johnny. Menanggapi hal tersebut, pakar keamanan siber Pratama Persada menilai hal tersebut merupakan pembelajaran yang sangat berharga.

Menurutnya, Tokopedia jelas bertanggung jawab atas kebocoran data pengguna yang dikuasai nya, dan wajar jika banyak pihak yang menggunakan data tersebut untuk tujuan kriminal. “Ini membuktikan bahwa Tokopedia memang diretas, berbeda dengan klaim Tokopedia sebelumnya yang menyatakan hanya ada satu peretasan di platform tersebut,” ujarnya. Meski gratis, namun mendownloadnya tidaklah mudah. File ini dihosting di server AS, sehingga pengguna harus menggunakan VPN dengan IP AS. Pratama menjelaskan, Raidforums memiliki mata uang tersendiri yang dapat digunakan oleh seluruh anggota yang mendaftar pertama kali.

Anggota dapat menyetor sejumlah minimal 8euro menggunakan layanan Paypal. Pengguna akan menerima 30 kredit ketika mengkonversi Rp 130.000. Orang yang juga Direktur Lembaga Penelitian Siber Cissrec Indonesia (Pusat Penelitian Keamanan Sistem Informasi dan Komunikasi) ini menambahkan, diperlukan pembayaran sebesar 8 EUR untuk memulihkan data 91 juta akun Tokopedia. Setelah selesai, pengguna akan diberikan tautan arsip pihak ketiga dan dapat mengunduhnya dalam format zip dengan ukuran data 9,5 GB. Setelah dekompresi, ukuran file akhir dalam format TXT akan menjadi 28,5 GB.

“Namun bukan berarti pengguna bisa membuka file teks sebesar itu. Pengguna memerlukan aplikasi khusus seperti Ultraedit untuk membukanya.” Kemudian, pengguna perlu memasukkan nama lengkap, nama akun, alamat email, secara online, Pengguna akan dapat melihat 91.174.216 data, termasuk toko, tanggal lahir", nomor ponsel, tanggal pendaftaran dan beberapa data yang dienkripsi dalam format hash," Pratama menjelaskan, fitur pencarian juga memudahkan untuk menemukan kata kunci email atau nomor telepon yang dicari pengguna. Berdasarkan link download data 91 juta akun Tokopedia, Minggu (5/7) pukul 10.00 WIB. masih dapat diakses dan telah diunduh oleh 58 anggota. Tautan mengatakan itu akan kedaluwarsa dalam 5 hari ke depan. Data yang diungkapkan tersebut sama dengan awal Mei 2020, yakni mulai Maret 2020.

"Undang - undang perlindungan data pribadi harus segera ditetapkan untuk mengatur sanksi dan teknik standar yang diterapkan kepada penyelenggara sistem elektronik," tegasnya. Pak Pratama menjelaskan, tanpa regulasi yang ketat, vendor sistem elektronik baik pemerintah maupun swasta tidak perlu menciptakan dan memelihara sistem terbaik nya. GDPR (Peraturan Perlindungan Data Umum) menjelaskan bagaimana peraturan turunannya memuat daftar teknologi yang berlaku dan jika terjadi pelanggaran data, peninjauan akan dilakukan dan sebaliknya akan melakukan litigasi. Jika terjadi kebocoran data, akan dilakukan audit dan jika tidak dilakukan, dapat diambil tindakan hukum senilai maksimal 20 juta euro atau sekitar Rp 320 miliar.

Implikasi dan dampak dari kasus kebocoran data Tokopedia terhadap konsumen dan perusahaan

Kaspersky mengumumkan pada hari Senin tanggal 5 April 2020 bahwa jenis pelanggaran data ini, jika tidak ditangani dengan benar, dapat menyebabkan kerugian reputasi dan finansial serta sanksi peraturan. Namun, jika penanganan data dikelola secara efektif, kerugian akibat pelanggaran data pelanggan dapat dikurangi secara signifikan. Sementara itu, laporan terbaru Kaspersky Lab, "Mengelola keamanan perusahaan dan privasi karyawan : Mengapa perlindungan siber penting bagi bisnis dan karyawan," menekankan "aspek kemanusiaan" dalam insiden keamanan siber. Laporan ini menguraikan akibat dan kerugian yang dialami karyawan akibat pelanggaran yang terjadi.

Sekitar sepertiga (30%) pekerja kantoran yang terkena dampak melewatkan acara pribadi yang penting, terpaksa bekerja shift malam (32%) dan bahkan mengalami stres yang lebih besar setelah sebuah insiden (33%). Seperempat dari mereka harus membatalkan liburan nya (27%). Meski pun risiko pelanggaran data selalu ada, bisnis harus mengelola keamanan data mereka untuk memastikan bahwa insiden tersebut tidak berdampak negatif terhadap kondisi kerja karyawan atau reputasi perusahaan, terutama selama pandemi COVID-19.

a) Tim IT Harus Bergerak

Ketika pelanggaran data terjadi, seluruh tim keamanan TI harus menyelidiki insiden tersebut, membersihkan dan memulihkan sistem, serta mengambil langkah - langkah untuk mencegah serangan tersebut terjadi lagi. Hasil : 1/3 manajer harus bekerja lembur di tempat kerja (33% di perusahaan kecil dan 32% di perusahaan besar). Bagi lebih dari seperempat usaha kecil (27%) dan korporasi (26%), hal ini juga dapat menunda pekerjaan lain atau menciptakan tenggat waktu yang ketat. Selain itu, hingga 20% staf TI bisnis kecil dan 30% staf TI perusahaan kehilangan kesempatan untuk merayakan pencapaian penting bersama, seperti ulang tahun orang tua atau makan bersama pasangan.

b) 29 Perusahaan Sulit Menarik Pelanggan Baru Usai Kena Bobol

Cara perusahaan menyimpan dan menggunakan data pelanggan berperan penting dalam membentuk dan mempertahankan reputasinya. Namun menurut studi Kaspersky, jenis data yang paling sering diserang oleh penjahat dunia maya adalah data pribadi (40%). Akibatnya, hingga 29% bisnis yang disurvei mengalami kesulitan menarik pelanggan baru setelah insiden kebocoran data. Untuk membantu pelanggan mengelola penanganan data dengan lebih baik, Kaspersky Lab telah memperluas platform pembelajaran kesadaran keamanan siber bagi bisnis dengan memasukkan kursus tentang Peraturan Perlindungan Data Umum (GDPR) dan data sensitif.

Untuk membantu bisnis memastikan bahwa kerja jarak jauh tidak menimbulkan risiko keamanan bagi bisnis mereka, Kaspersky Lab juga memperkenalkan modul gratis untuk keamanan dasar saat bekerja dari rumah. Kursus Data Sensitif mencakup aturan umum untuk menangani informasi sensitif, seperti informasi pribadi, rahasia dagang, dan dokumen internal yang tidak boleh dibagikan secara eksternal. Topik baru ini akan membantu pengguna membekali karyawan dengan keterampilan yang diperlukan untuk bekerja dengan sumber informasi ini dan mempelajari cara meminimalkan kerusakan jika terjadi pelanggaran data.

Upaya penanganan dan tanggapan pihak berwenang

a) Cara Tokopedia mengatasi kebocoran data pribadi

Perusahaan e-commerce Tokopedia kehilangan 91 juta data pengguna pada Mei lalu. CEO Tokopedia William Tanuwijaya mengaku pihaknya telah menyiapkan banyak cara untuk memperbaiki kebocoran tersebut. "Indonesia tidak memiliki peraturan untuk melindungi data pribadi, jadi kami mengikuti praktik terbaik standar global untuk mengatasi pelanggaran data," kata William saat sidang panel IR (RDP) ke-6 DPR RI, Rabu, 15 September. transparansi dengan menyampaikan seluruh data yang bocor kepada pengguna. Kedua, memberi tahu pengguna tentang kemajuan pengobatan. Ketiga, kami akan berupaya memperbaiki struktur internal kami.

Terakhir, berkoordinasi dengan pemerintah dan pihak berwenang terkait insiden pelanggaran data. Pada Mei tahun lalu, hingga 91 juta data pengguna Tokopedia bocor di forum hacker dan tersedia untuk diunduh gratis. Setelahnya, Tokopedia melaporkan kebocoran data pengguna tersebut ke polisi. Namun William mengatakan pelanggaran tersebut bukan karena kesalahan perusahaan dalam menangani data pribadi pengguna. "Sebagian besar yang terjadi didasarkan pada asumsi bahwa platform ini tidak memberikan perlindungan," katanya.

Ia mengatakan masyarakat harus membedakan antara aktivitas kejahatan siber yang dilakukan peretas dan kelalaian perusahaan dalam menangani data pribadi. Terkait dengan kejahatan dunia maya, sebagian besar terjadi di dalam gedung.

"Bahkan Pentagon pun di bobol," kata William. William mendesak pihak - pihak terkait untuk merancang peraturan untuk mengendalikan kejahatan dunia maya dan menerapkan hukuman yang berat. Namun pembahasan Undang - Undang Perlindungan Data Pribadi (RUU PDP) di DPR masih terhenti karena adanya kesepakatan dan kebuntuan yang melibatkan otoritas pengawas.

DPR berharap RUU PDP bisa mengatur pembentukan lembaga independen di bawah naungan presiden untuk memantau pelanggaran data pribadi. Lebih lanjut, Kementerian Informasi dan Komunikasi (Kominfo) menegaskan kewenangan tersebut merupakan kewenangan Kementerian. Padahal, pada Maret lalu, RUU PDP diperkirakan baru bisa disahkan pada Mei setelah Idul Fitri. Bahkan, target tersebut sempat mengalami penundaan beberapa kali dibandingkan rencana awal tahun 2019.

Penyelesaiannya kemudian dijadwalkan pada November 2020. Penyelesaiannya kemudian ditunda hingga Desember 2020 dan kemudian Maret 2021. Pratama Persada, peneliti keamanan siber di Center for Research Communications and Information Systems Security Research (CISSReC), mengatakan RUU PDP harus segera diselesaikan. "Cukup mempertimbangkan untung ruginya perbedaan pendapat bagi regulator. "Tapi ini harus dilakukan dari sudut pandang obyektif," ujarnya pada Juli lalu (8 Juli).

b) Tanggapan pihak Kementerian Kominfo

Kementerian Informasi dan Komunikasi meminta perusahaan pengelola platform digital Tokopedia melakukan investigasi internal. Tujuannya adalah untuk mengidentifikasi dugaan pelanggaran perlindungan data pada platform marketplace dan mengambil tindakan yang diperlukan untuk menjamin keamanan data pengguna. Sebelumnya, Tokopedia mengaku berencana meretas data pengguna. Tindakan ini menyusul adanya permasalahan yang melibatkan 15 juta data pengguna Tokopedia yang dibobol. "Kami menulis artikel dan melakukan voting di Tokopedia.

Menteri Informasi dan Komunikasi Johnny G. Plate di Jakarta, Minggu, 3 Mei 2020 mengatakan : "Tim teknis Kominfo telah melakukan penyesuaian teknis untuk memantau masalah pelanggaran data pengguna". Hal - hal untuk memastikan keamanan data pengguna. "Hal pertama yang harus dilakukan Tokopedia adalah segera mengamankan sistem nya untuk mencegah pelanggaran data yang meluas. Selanjutnya, Tokopedia akan memberi tahu pemegang akun yang informasi pribadinya mungkin telah di bobol.

Dan ketiga, kami melakukan investigasi internal untuk memastikan dugaan pelanggaran data dan jika terjadi pelanggaran data, cari penyebabnya, jelasnya. Menteri Johnny mengatakan Kementerian

Informasi dan Komunikasi telah meminta untuk memberi tahu pemegang akun tentang dugaan pelanggaran data, tindakan keamanan sistem yang diambil, dan laporan kemungkinan dampak pelanggaran data terhadap pemilik data. "Kami masih menunggu laporannya selesai," ujarnya. Sebagai Penyelenggara Sistem Elektronik (ESO), Tokopedia harus mematuhi standar pengamanan yang tertuang dalam Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik serta Peraturan Kementerian Komunikasi dan Informatika Nomor 20 Tahun 2016.

Perlindungan subjek data dan data pribadi dalam sistem elektronik. "Tokopedia mengatakan sistem keamanannya menggunakan kata sandi yang disimpan dalam bentuk hash. "Selain itu, Tokopedia menggunakan fungsi OTP sebagai autentikasi dua faktor sehingga pengguna selalu diminta memasukkan kode baru secara real time setiap kali login." Dia menjelaskan. Kementerian Informasi dan Komunikasi juga mengimbau masyarakat untuk memastikan keamanan akun mereka.

Menkominfo menekankan : "Masyarakat harus rutin mengganti password dan tidak mudah percaya kepada siapapun yang meminta password atau kode OTP." Menurut Sekretaris Johnny, password dan OTP hanya diperlukan untuk sistem. Oleh karena itu, jika permintaan password atau OTP dilakukan oleh perorangan, pada hakikatnya itu adalah penipuan, tegasnya. Menkominfo juga mewanti - wanti adanya penipuan phising dan phising yang bertujuan memancing masyarakat untuk mencuri akun pribadinya.

"Ada banyak penipuan akhir-akhir ini. Sebelum mengklik tautan yang diterima pengguna melalui email, pastikan alamat email pengirimnya asli. "Cara membacanya dari belakang ke depan," jelasnya. Menkominfo menambahkan, Kemenkominfo akan mengundang direksi Tokopedia. Terkait permasalahan ini, saya meminta CEO Aptica memanggil jajaran direksi Tokopedia untuk memberikan pernyataan terkait hal tersebut. "Pertemuan akan dilakukan pada Senin, 4 Mei," ujarnya.

Segera bahas RUU PDP

Saat ini dugaan pembobolan data akun pengguna Tokopedia ditangani berdasarkan Undang - Undang Informasi dan Transaksi Elektronik (ITE) dan Peraturan Pemerintah Nomor 71 Tahun 2019. Sementara itu, pemerintah bersama Dewan Perwakilan Rakyat (DPR) terus berupaya untuk membenahi data akun pengguna Tokopedia. Mempercepat pengesahan RUU Perlindungan Data Pribadi (RUU). Diketahui, Pemerintah telah mengirimkan surat Presiden (Supres) ke DPR terkait UU PDP. Dan kini sedang berlangsung proses politik di DPR.

"Pemerintah melalui Kementerian Informasi dan Komunikasi juga sedang menyiapkan panitia kerja yang berkoordinasi dengan DPR untuk mendorong proses ini. Kami yakin pemerintah dan DPR akan terus memprioritaskan pengesahan UU PDP. Menteri Johnny menyimpulkan, "Apalagi RUU ini masuk dalam Program Legislatif Nasional (Prolegnas) Prioritas.

Prioritas keamanan data dan privasi pengguna

Ekhel Chandra Wijaya, Head of Corporate Affairs Tokopedia, mengatakan privasi pengguna menjadi prioritas utama Tokopedia. "Tokopedia sebagai perusahaan teknologi Indonesia yang berbasis kepercayaan tetap berkomitmen menjaga keamanan sistem teknologi informasi (TI) serta melindungi dan menjaga privasi data pengguna," kata Eker, Selasa (5 Februari). Ekhel mengatakan Tokopedia mengambil pendekatan tiga arah untuk menjaga keamanan sistem TI - nya dan melindungi data dan privasi pengguna, termasuk manusia, proses, dan teknologi. Tokopedia memiliki tim Keamanan Sistem IT (IT Security Office) dan tim DPPO (Data Protection and Data Protection Office), dan Ekhel mengatakan tim - tim ini secara khusus bertanggung jawab atas keamanan sistem IT dan memastikan sistem aman dan terlindungi dalam proses ini. Kita perlu memperkuat ekosistem digital terpercaya kita.

Selain itu, pengelolaan sistem perlindungan informasi dan perlindungan data Tokopedia telah di sertifikasi secara internasional oleh Organisasi Internasional untuk Standardisasi (ISO). Ekhel mengatakan, aktivitas Tokopedia sudah sesuai standar perdagangan internasional karena Tokopedia

sudah mengantongi sertifikasi ISO 27001 untuk keamanan informasi dan sertifikasi ISO 27701 untuk pengelolaan informasi. Perlindungan ini juga disertakan dalam metode pembayaran pengguna. Ia menambahkan, keamanan dan ketahanan sistem metode pembayaran Tokopedia telah diakui memenuhi standar industri tertinggi. Ekhel membenarkan metode pembayaran Tokopedia telah meraih sertifikasi PCI DSS Level 1, sertifikasi keamanan kartu kredit tingkat tertinggi.

Selain itu, Tokopedia juga bekerja sama dengan mitra strategis antara lain pakar keamanan sistem IT, pakar perlindungan data pribadi, konsultan, dan penggiat industri teknologi lainnya. Menurut Ekhel, tujuannya adalah untuk meningkatkan kualitas prosedur dalam memprediksi dan mencegah ancaman terhadap keamanan sistem TI. Penilaian tahunan dilakukan oleh tim internal Tokopedia dan pihak ketiga untuk mengukur dan memvalidasi kinerja kemampuan keamanan sistem TI yang ada dan memastikan memenuhi praktik terbaik global dan standar industri. Tokopedia menggunakan teknologi untuk terus meningkatkan praktik keamanan sistem TI - nya, melindungi data pengguna melalui teknologi otomatisasi, deteksi, dan respons, serta melayani berbagai kebutuhan. “Kami juga menerapkan prinsip privacy by design saat menganalisis dan menilai kesiapan perlindungan data dan privasi pengguna setiap kali kami meluncurkan dan atau memperbarui produk atau fitur yang melibatkan penggunaan data pribadi (Privacy Impact Assessment),” jelas Ekel.

Tokopedia juga terus memperkuat keamanan platform di seluruh cloud, endpoint, dan aplikasi, menerapkan serangkaian prinsip keamanan sistem TI sesuai dengan standar keamanan industri tertinggi. Ekhel menegaskan, ada beberapa poin keamanan data yang bisa diambil oleh pengguna Tokopedia. Langkah - langkah tersebut antara lain memastikan pengguna selalu mengganti kata sandi akun Tokopedia secara berkala, menghindari penggunaan kata sandi yang sama di berbagai platform digital, dan melindungi kata sandi satu kali (OTP) dengan tidak membagikan kode OTP kepada pihak mana pun. Selain itu, Anda harus berhati - hati saat mengunjungi situs tidak resmi, menanggapi pesan, dan membuka lampiran yang dikirim atas nama Tokopedia. Sebagai pengingat, Ekhel mengingatkan pengguna untuk membaca privasi dan kebijakan privasi Tokopedia.

Keamanan data masih menjadi isu sensitif sehingga memberikan tantangan baru bagi perusahaan digital untuk menciptakan ekosistem yang terlindungi dari serangan peretas yang tidak bertanggung jawab. Menurut data Fortinet, hingga 94% bisnis mengalami pelanggaran atau pencurian data tahun ini.

Dampak dari kebocoran data terhadap perspektif konsumen

Kebocoran data di Tokopedia atau platform bisnis online lainnya dapat berdampak signifikan terhadap persepsi konsumen terhadap bisnis online. Potensi dampaknya mencakup perubahan kepercayaan konsumen, aktivitas pengguna, reputasi perusahaan, litigasi, dan kebijakan keamanan data.

a. Ketidakpercayaan konsumen: Pelanggaran data dapat merusak kepercayaan konsumen terhadap keamanan dan privasi datanya. Konsumen mungkin menjadi skeptis dalam memperdagangkan atau berbagi data pribadi pada platform tersebut.
b. Lebih sedikit pengguna aktif: Konsumen yang mengkhawatirkan keamanan datanya cenderung mengurangi aktivitasnya atau berhenti menggunakan platform. Penurunan jumlah pengguna aktif dapat berdampak negatif terhadap kestabilan bisnis online.
c. Hilangnya reputasi : Perusahaan online yang mengalami pelanggaran data dapat terus mengalami kerusakan reputasi. Persepsi negatif konsumen terhadap keamanan data dapat berdampak negatif terhadap citra merek dan sulit untuk dipulihkan.
d. Tuntutan Hukum : Pelanggaran data seringkali diikuti dengan tuntutan hukum dari konsumen yang merasa terhina. Perusahaan online mungkin menghadapi konsekuensi hukum seperti sanksi dan denda, yang dapat menimbulkan konsekuensi finansial.
e. Meningkatkan Keamanan Data : Untuk mendapatkan kembali kepercayaan konsumen dan mematuhi peraturan, bisnis online harus meningkatkan keamanan data. Hal ini mungkin

memerlukan investasi tambahan dalam teknologi keamanan dan penerapan praktik keamanan yang lebih ketat.

Penting bagi pebisnis online untuk mengambil tindakan proaktif untuk mengatasi dampak negatif. Hal ini termasuk meningkatkan keamanan data, memberikan informasi yang transparan kepada konsumen, menangani litigasi dengan serius, dan mengkomunikasikan dengan jelas perubahan kebijakan keamanan data kepada pengguna. Transparansi dan akuntabilitas dapat membantu memulihkan kepercayaan konsumen dan meminimalkan dampak jangka panjang terhadap bisnis online.

KESIMPULAN

Menanggapi pelanggaran data tersebut, perusahaan media dan IT Johnny Gerald Plate meminta direktur platform digital Tokopedia untuk melakukan penyelidikan internal. Tujuannya adalah untuk mengidentifikasi dugaan pelanggaran perlindungan data pada platform marketplace dan mengambil tindakan yang diperlukan untuk menjamin keamanan data pengguna. “Ditulis bekerja sama dengan Tokopedia. Johnny mengatakan pada Minggu, 3 Mei 2020, tim teknis Kominfo melakukan penyesuaian teknis untuk memantau permasalahan pelanggaran data pengguna, mengutip siaran pers Kementerian Informasi dan Komunikasi Jakarta Media.

Johnny mengatakan Kementerian Informasi dan Komunikasi meminta Tokopedia melakukan tiga hal untuk menjamin keamanan data pengguna. “Hal pertama yang harus dilakukan Tokopedia adalah segera mengamankan sistem nya untuk mencegah pelanggaran data yang meluas. Kami kemudian akan memberi tahu pemegang akun yang informasi pribadinya mungkin telah di bobol. Dan ketiga, kami melakukan investigasi internal untuk memastikan dugaan pelanggaran data dan jika terjadi pelanggaran data, cari penyebabnya, jelasnya.

DAFTAR PUSTAKA

https://www.cnbcindonesia.com/tech/20200504063854-37-155936/cerita-lengkap-bocornya-91-juta-data-akun-tokopedia

https://teknologi.bisnis.com/read/20200503/84/1235695/pembobolan-data-tokopedia-ini-dampak-ke-konsumen

https://www.jawapos.com/teknologi/01277505/91-juta-data-akun-tokopedia-bocor-dan-disebar-di-forum-internet

https://www.liputan6.com/tekno/read/4244527/tokopedia-diserang-hacker-ini-dampak-bagi-karyawan-dan-pelanggan

https://katadata.co.id/lavinda/digital/61421ec0427f1/tokopedia-ungkap-cara-atasi-kasus-kebocoran-data-pribadi

https://www.kominfo.go.id/content/detail/26247/siaran-pers-no-63hmkominfo052020-tentang-demi-melindungi-data-pengguna-kominfo-minta-tokopedia-lakukan-investigasi-internal/0/siaran_pers

https://bisnis.solopos.com/tak-perlu-takut-bocor-tokopedia-pastikan-keamanan-privasi-data-pengguna-1615628

https://www.cnbcindonesia.com/tech/20200504063854-37-155936/cerita-lengkap-bocornya-91-juta-data-akun-tokopedia/2