LATIHAN KELOMPOK

ANALISIS STUDI KASUS KEBOCORAN DATA TOKOPEDIA

Oleh :

Daffa DzulFaqor Dhiya Ulhaq – F1E123023

Ahmad Fadlan – F1E123077

Muhammad Rizkon Adhol – F1E123081

Desti Amanda – F1E123021

Zahra Zahira – F1E123089

Aktavia Putri Irena – F1E123057

Fitri Agustina – F1E123091

Aisyah Putri Hasbi – F1E123097

A. Pendahuluan

Pada Mei 2020, Tokopedia, salah satu platform e-commerce terbesar di Indonesia, mengalami kebocoran data yang melibatkan informasi pribadi lebih dari 91 juta pengguna. Data yang bocor mencakup nama, email, nomor telepon, tanggal lahir, dan kata sandi yang telah di-hash. Kebocoran ini menjadi perhatian serius karena data tersebut dilaporkan diperjualbelikan di forum dark web, memicu kekhawatiran terkait privasi dan keamanan pengguna. Kasus ini menunjukkan betapa pentingnya pengelolaan dan perlindungan data dalam era digital, terutama bagi perusahaan dengan basis pengguna yang besar. Analisis ini akan membahas bagaimana serangan terjadi, dampaknya terhadap pengguna, serta langkah-langkah pencegahan yang dapat diambil untuk menghindari kejadian serupa.

B. Analisis Kasus

1. Penyebab Kejadian

   Kebocoran data Tokopedia pada 2020 disebabkan oleh peretasan yang dilakukan oleh hacker bernama Whysodank, yang mengungkapkan hasil peretasan di forum RaidForums. Peretasan terjadi pada 20 Maret 2020 dan melibatkan 91 juta akun pengguna serta 7 juta akun merchant. Data yang bocor termasuk nama, email, dan nomor telepon, dijual di dark web seharga $5,000. Meskipun Tokopedia menyatakan bahwa password pengguna tetap terlindungi, insiden ini menunjukkan kelemahan dalam sistem keamanan mereka dan menimbulkan risiko bagi pengguna yang menggunakan email dan password yang sama di berbagai platform.

2. Celah Keamanan yang Dimanfaatkan
    - Misalnya mengirimkan link phising maupun upaya social engineering lainnya, karena itu seharusnya Tokopedia melakukan update dan informais kepada seluruh penggunanya segera
    - Serangan SQL Injection: Metode lain yang mungkin digunakan adalah serangan SQL injection, di mana peretas menyisipkan kode berbahaya ke dalam query database untuk mendapatkan akses tidak sah ke data.

C. Dampak Insiden

1. Dampak Finansial, Operasional, dan Reputasi
    - Finansial : Tokopedia menghadapi gugatan senilai Rp 100 miliar dari KKI, Tokopedia harus menginvestasikan dana besar untuk memperkuat sistem keamanan, memperbaiki kerentanan, dan mengelola krisis, termasuk menyewa tim ahli keamanan siber, Kepercayaan konsumen yang menurun dapat mengurangi transaksi di platform, yang pada akhirnya memengaruhi pendapatan Tokopedia.

    - Operasional: Perusahaan harus meningkatkan sistem keamanan dan melatih karyawan tentang perlindungan data, yang dapat mengalihkan fokus dari inovasi dan pertumbuhan, Investigasi kebocoran data dapat menyita sumber daya perusahaan, termasuk waktu dan tenaga karyawan, sehingga mengganggu operasional sehari-hari, Tokopedia harus mengimplementasikan pembaruan prosedur keamanan, seperti memperketat autentikasi pengguna, enkripsi data, dan audit keamanan berkala.

    - Reputasi : Kejadian ini merusak citra Tokopedia sebagai platform yang aman, Kejadian ini menyebabkan kerugian reputasi, di mana 29% perusahaan mengalami kesulitan menarik pelanggan baru setelah pelanggaran data, Selain itu, memicu kekhawatiran di kalangan pengguna dan mengurangi loyalitas pelanggan, berpotensi mempengaruhi pangsa pasar

2. Dampak Terhadap Pengguna atau Nasabah

    1. Pelanggaran Privasi

    Informasi pribadi seperti nama, email, nomor telepon, dan tanggal lahir pengguna yang bocor membuka peluang bagi pihak tak bertanggung jawab untuk menyalahgunakan data tersebut. Hal ini dapat menciptakan rasa tidak aman di kalangan pengguna karena data mereka tidak lagi bersifat rahasia.

    2. Ancaman Phishing dan Penipuan

    Data yang bocor memudahkan pelaku kejahatan siber melakukan serangan phishing. Dengan informasi seperti email atau nomor telepon, pelaku dapat mengirimkan pesan palsu yang tampak resmi untuk menipu pengguna agar memberikan data tambahan seperti kode OTP, informasi kartu kredit, atau akses ke akun lainnya.

    3. Potensi Pembobolan Akun

Meskipun kata sandi yang bocor telah di-hash, pelaku dengan kemampuan teknis dapat mencoba mendekripsi hash tersebut. Jika pengguna menggunakan kata sandi yang sama di berbagai platform, risiko pembobolan akun menjadi lebih tinggi.

4. Kerugian Finansial
Kebocoran data ini dapat dimanfaatkan untuk akses ilegal ke akun pengguna yang terhubung dengan metode pembayaran, seperti kartu kredit atau e-wallet. Selain itu, pengguna juga dapat menjadi target penipuan yang berdampak langsung pada kerugian finansial.

5. Penurunan Kepercayaan
Kasus ini menimbulkan ketidakpercayaan terhadap Tokopedia sebagai penyedia layanan e-commerce. Banyak pengguna menjadi ragu untuk terus menggunakan platform ini, khawatir data mereka akan kembali terancam.

6. Potensi Penyalahgunaan Data di Dark Web
Data pengguna yang bocor dilaporkan diperjualbelikan di forum dark web. Hal ini membuka peluang bagi pihak lain untuk menyalahgunakan informasi tersebut untuk berbagai kejahatan, seperti pencurian identitas, pemalsuan dokumen, atau tindakan kriminal lainnya.

D. Solusi dan Rekomendasi

1. Solusi Teknis
   1. Peningkatan Keamanan Data:
   Implementasi enkripsi menyeluruh pada semua data sensitif, bukan hanya password. Data seperti user ID, email, dan nomor telepon harus dilindungi dengan enkripsi tingkat tinggi.
   Melakukan pembaruan keamanan (security patch) secara berkala untuk mengurangi kerentanan sistem.

   2. Pemantauan dan Investigasi:
   Melacak aktivitas login dan logout yang mencurigakan serta memeriksa log server untuk menganalisis sumber serangan.
   Bekerja sama dengan pihak berwenang untuk mengidentifikasi pelaku melalui investigasi mendalam.

   3. Penguatan Infrastruktur IT:
   Menambahkan beberapa lapisan keamanan (multi-layered security) untuk perlindungan data pribadi.
   Menggunakan vendor teknologi atau ahli keamanan siber yang teruji dan berpengalaman untuk mendukung sistem.

2. Kebijakan Organisasi yang perlu diadopsi
   1. Kebijakan organisasi yang perlu diadopsi Kebocoran Data Tokopedia (2020)

melakukan upaya perbaikan sistem secara
berkoordinasi dengan dengan pemerintah dan berbagai pihak berwenang terkait insiden kebocoran data tersebut.

2. Kebijakan Manajemen Risiko Keamanan Siber
Penilaian Risiko Rutin: Melakukan analisis risiko secara berkala untuk mengidentifikasi potensi kerentanan.
Pengujian Keamanan Sistem: Melakukan penetration testing dan vulnerability assessment secara teratur.
Protokol Tanggap Insiden: Menyusun rencana tanggap darurat yang jelas untuk merespons dan memitigasi dampak kebocoran data.

3. Kebijakan Privasi Data
Minimasi Data: Mengumpulkan dan menyimpan hanya data yang diperlukan untuk operasional bisnis.
Hak Akses Terbatas: Menerapkan prinsip "least privilege" untuk akses data pengguna, sehingga hanya pihak yang benar-benar memerlukan dapat mengaksesnya.
Pseudonimisasi: Menggunakan pseudonimisasi untuk melindungi data pengguna.

3. Rencana Pemulihan setelah serangan
Rencana pemulihan setelah serangan kebocoran data di Tokopedia pada tahun 2020 sebaiknya melibatkan beberapa langkah yang bertujuan untuk memitigasi kerusakan dan mencegah kejadian serupa di masa depan. Berikut adalah beberapa langkah penting yang dapat diambil dalam rencana pemulihan:

1. Identifikasi dan Analisis Kejadian:
Melakukan audit menyeluruh untuk memahami skala kebocoran data dan mengidentifikasi informasi apa saja yang terungkap (misalnya, nama pengguna, email, kata sandi, dan data lainnya).
Menyusun laporan kejadian untuk memberi transparansi kepada pihak berwenang, pemangku kepentingan, dan pelanggan.

2. Komunikasi kepada Pengguna dan Pemangku Kepentingan:
Memberikan pemberitahuan kepada pengguna yang terdampak oleh kebocoran, termasuk tindakan yang dapat mereka ambil, seperti mengganti kata sandi.
Menyediakan panduan keamanan dan pencegahan lebih lanjut untuk pengguna.
Memberitahu pihak berwenang dan regulator sesuai dengan kewajiban yang ada, jika diperlukan oleh hukum.

3. Peningkatan Keamanan Sistem:
Menilai dan memperbarui sistem keamanan, termasuk enkripsi data, penggunaan kata sandi yang lebih kuat, dan sistem otentikasi dua faktor (2FA).
Menerapkan pemantauan dan deteksi intrusi yang lebih baik untuk mendeteksi serangan lebih dini di masa depan.
Melakukan uji penetrasi (penetration testing) untuk mengidentifikasi celah yang belum ditemukan sebelumnya.

4. Peningkatan Prosedur Keamanan dan Pelatihan:
Meningkatkan pelatihan bagi karyawan tentang prosedur keamanan dan langkah-langkah pencegahan untuk menghindari kebocoran data di masa depan.
Memperkenalkan kebijakan pengelolaan data yang lebih ketat dan pembatasan akses data sesuai dengan prinsip kebutuhan yang jelas.

5. Evaluasi Infrastruktur TI dan Kerja Sama dengan Pihak Ketiga:
Menilai infrastruktur TI dan periksa apakah ada komponen atau mitra pihak ketiga yang terlibat dalam kebocoran.
Jika ada pihak ketiga yang turut berperan, bekerjasama untuk memastikan bahwa mereka juga meningkatkan langkah-langkah keamanan mereka.

6. Pemulihan Reputasi:
Mengelola dampak reputasi dengan menjalankan program komunikasi dan transparansi yang berkelanjutan, menjelaskan langkah-langkah yang diambil untuk memperbaiki dan mencegah insiden serupa.
Menawarkan kompensasi atau layanan tambahan kepada pelanggan yang merasa dirugikan, seperti layanan pemantauan identitas atau kredit perlindungan.

7. Pemantauan dan Penyesuaian Berkelanjutan:
Memastikan pemantauan berkelanjutan terhadap keamanan data dan menyesuaikan kebijakan berdasarkan tren ancaman baru dan teknologi yang berkembang.

E. Kesimpulan

Kasus kebocoran data Tokopedia pada Mei 2020 menunjukkan betapa krusialnya pengelolaan dan perlindungan data pribadi dalam era digital, terutama bagi platform besar yang mengelola jutaan pengguna. Kebocoran yang melibatkan informasi pribadi lebih dari 91 juta pengguna, yang termasuk nama, email, nomor telepon, dan tanggal lahir, disebabkan oleh serangan peretasan yang memanfaatkan celah keamanan di sistem Tokopedia. Insiden ini tidak hanya berdampak finansial, operasional, dan reputasi bagi perusahaan, tetapi juga menimbulkan ancaman serius bagi pengguna, seperti pelanggaran privasi, potensi penipuan melalui phishing, serta pembobolan akun.

Dalam menanggapi insiden ini, Tokopedia harus melakukan langkah-langkah perbaikan yang meliputi peningkatan sistem keamanan dengan enkripsi data yang lebih baik, pemantauan aktivitas mencurigakan, serta penggunaan infrastruktur IT yang lebih kuat. Selain itu, penting bagi perusahaan untuk menerapkan kebijakan organisasi yang lebih ketat terkait perlindungan data dan bekerja sama dengan pihak berwenang. Untuk pemulihan, Tokopedia perlu melakukan komunikasi transparan kepada pengguna, memperbaiki prosedur keamanan, dan menawarkan kompensasi atau layanan tambahan untuk mengembalikan kepercayaan pengguna.

Secara keseluruhan, kasus ini menggarisbawahi pentingnya upaya berkelanjutan dalam menjaga keamanan data pribadi pengguna dan meningkatkan sistem perlindungan data yang adaptif terhadap ancaman siber yang terus berkembang.

F. Referensi

(t.thn.). Diambil kembali dari https://www.cnbcindonesia.com/tech/20200507083340-37-156876/91-juta-data-pengguna-bocor-tokopedia-digugat-rp-100-m/2

(t.thn.). Diambil kembali dari https://www.cnnindonesia.com/teknologi/20200506105640-185-500591/6-bahaya-yang-intai-usai-kasus-data-bocor-tokopedia-bukalapak

(t.thn.). Diambil kembali dari https://jurnal.unmer.ac.id/index.php/blj/article/download/5850/pdf

(t.thn.). Diambil kembali dari https://journal.moestopo.ac.id/index.php/pustakom/article/download/2186/1074

(t.thn.). Diambil kembali dari https://inet.detik.com/security/d-5083013/bagaimana-hacker-curi-data-pengguna-tokopedia

(t.thn.). Diambil kembali dari https://katadata.co.id/digital/e-commerce/61421ec0427f1/tokopedia-ungkap-cara-atasi-kasus-kebocoran-data-pribadi

(t.thn.). Diambil kembali dari http://tirto.id/91-juta-data-pengguna-tokopedia-bocor-dan-disebar-di-forum-internet-fNH1

(t.thn.). Diambil kembali dari https://news.republika.co.id/berita/q9t9o7409/kasus-tokopedia-dan-perlunya-uu-perlindungan-data-pribadi#google_vignette