# LAPORAN ANALISIS KEJAHATAN SIBER

## Identitas Pelapor

Nama : Adam Ghonifirlandi

NIM : 233140707111102

## A. Informasi Kasus

• Judul Kasus : kebocoran data 91 Juta Akun Tokopedia

• Tahun Kejadian : 2020

• Lokasi : Tokopedia (Indonesia)

• Jenis Serangan : data breach

• Pihak yang Terlibat : Tokopedia selaku korban dan untuk pelaku belum teridentifikasi

• Sumber Referensi : <https://www.cnnindonesia.com/teknologi/20200503153210-185->499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual

## B. Analisis Penyebab Insiden *[nilai 30]*

### 1. Faktor Teknis

Tokopedia mengalami kebocoran data besar karena beberapa kelemahan teknis. Enkripsi data yang tidak memadai membuat pelaku bisa membaca dan mengakses data pengguna dengan mudah. Autentikasi sistem yang tidak kuat membuat pelaku bisa mendapatkan akses ke sistem Tokopedia tanpa harus memiliki izin yang sah. Pengamanan jaringan yang tidak memadai membuat pelaku bisa mendapatkan akses ke jaringan Tokopedia dan mengakses data pengguna.

Kelemahan-kelemahan ini membuat pelaku bisa mendapatkan akses ke data pengguna, menyebabkan kehilangan kepercayaan pelanggan, kerugian finansial, dan kehilangan reputasi.

### 2. Faktor Manusia

Kesalahan manusia dalam kasus serangan siber Tokopedia disebabkan oleh beberapa faktor, yaitu kurangnya kesadaran dan pemahaman tentang keamanan siber, yang berdampak pada kurangnya disiplin dan konsistensi dalam mengikuti prosedur keamanan. Hal ini diperburuk oleh kurangnya komunikasi dan koordinasi antar tim, serta kurangnya pelatihan dan pengembangan keterampilan, sehingga memungkinkan pelaku untuk menemukan celah keamanan dan melakukan serangan siber yang lebih efektif.

### 3. Faktor Prosedural

Kurangnya kebijakan keamanan yang jelas dan efektif di Tokopedia menyebabkan beberapa kelalaian prosedural. Antara lain, prosedur autentikasi dan autorisasi yang lemah memungkinkan akses tidak sah ke sistem dan data. Selain itu, kurangnya prosedur pengelolaan akses dan perubahan menyebabkan akses pengguna tidak diatur dan dipantau secara ketat. Akhirnya, kurangnya prosedur pengelolaan insiden membuat Tokopedia tidak siap untuk menghadapi dan menangani insiden keamanan.

## C. Analisis Risiko *[nilai 10]*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No | Risiko | Probability | Impact | Skor Risiko (P x I) |
| 1 | Kebocoran Data | [High] | [High] | [9] |
| 2 | [gangguan operasional] | [Medium] | [Medium] | [6] |
| 3 | [kerugian finansial] | [High] | [High] | [9] |

## D. Analisis Dampak terhadap Perusahaan *[nilai 40]*

### 1. Dampak Finansial

### Menurut laporan, serangan siber pada Tokopedia pada tahun 2020 mengakibatkan kebocoran data pengguna sebanyak 91 juta akun. Dampak kerugian finansial dari serangan ini dapat diestimasi sebagai berikut :

* Biaya penggantian dan pemulihan data: Rp 100 miliar - Rp 500 miliar
* Biaya peningkatan keamanan sistem: Rp 50 miliar - Rp 200 miliar
* Biaya kompensasi kepada pengguna yang terkena dampak: Rp 100 miliar - Rp 500 miliar
* Biaya reputasi (tidak diketahui jumblahnya)

### Dengan demikian, estimasi total dampak kerugian finansial akibat serangan siber pada Tokopedia dapat mencapai Rp 350 miliar - Rp 1,4 triliun. Namun, perlu diingat bahwa estimasi ini hanya berdasarkan pada beberapa aspek dan mungkin tidak mencakup semua biaya yang terkait dengan serangan siber ini.

### 2. Dampak Operasional

### Serangan siber pada Tokopedia berdampak signifikan pada operasional perusahaan. Layanan Tokopedia harus dihentikan sementara untuk memperbaiki kerentanan keamanan dan memulihkan data. Proses bisnis, seperti pengolahan transaksi dan pengiriman barang, juga terganggu. Karyawan Tokopedia harus fokus pada pemulihan sistem dan data, sehingga mengurangi produktivitas dan efisiensi kerja. Tokopedia juga harus mengalokasikan sumber daya tambahan untuk mengatasi dampak serangan siber. Selain itu, hubungan dengan mitra dan supplier juga terganggu, mempengaruhi kemampuan perusahaan untuk memenuhi kebutuhan pelanggan.

### 3. Dampak Reputasi

### Serangan siber pada Tokopedia berdampak signifikan pada reputasi perusahaan. Pelanggan kehilangan kepercayaan pada Tokopedia dan merasa tidak aman. Reputasi merek Tokopedia rusak dan persepsi pelanggan terhadap perusahaan memburuk. Akibatnya, pendapatan Tokopedia terpengaruh dan kepercayaan investor pada perusahaan juga terganggu. Selain itu, serangan siber ini juga memberikan keuntungan pada kompetitor Tokopedia dan mempengaruhi posisi pasar perusahaan. Dengan demikian, serangan siber ini memiliki dampak yang luas dan signifikan pada reputasi dan keseluruhan bisnis Tokopedia.

### 4. Dampak Regulasi dan Hukum

Serangan siber pada Tokopedia berdampak signifikan pada aspek regulasi dan hukum. Perusahaan dapat dikenakan sanksi oleh otoritas regulasi seperti Kominfo dan OJK karena tidak memenuhi standar keamanan data. Selain itu, pelanggan yang terkena dampak serangan siber dapat menggugat Tokopedia karena tidak menjaga keamanan data mereka. Tokopedia juga dapat kehilangan izin operasional jika tidak memenuhi standar keamanan data. Biaya hukum dan regulasi yang dikeluarkan oleh Tokopedia juga dapat membengkak. Pada akhirnya, dampak regulasi dan hukum ini dapat mempengaruhi reputasi dan kepercayaan pelanggan pada Tokopedia.

Meskipun begitu Tokopedia tidak dikenakan sanksi hukum secara langsung atas kebocoran data pengguna yang terjadi pada Mei 2020. Namun, perusahaan tersebut dituntut melakukan beberapa tindakan untuk memperbaiki sistem keamanan dan meminimalkan dampak kebocoran data.

## E. Rekomendasi dan Mitigasi *[nilai 10]*

|  |  |  |  |
| --- | --- | --- | --- |
| No | Tindakan Pencegahan | Prioritas | Teknologi/Pendekatan |
| 1 | Implementasi Autentikasi Dua Faktor (2FA) | Tinggi | Google Authenticator, Authy |
| 2 | Penggunaan Enkripsi Data | Tinggi | AES, RSA |
| 3 | Pembaruan Sistem Keamanan | Sedang | Pembaruan otomatis, Nessus, OpenVAS |

## F. Kesimpulan *[nilai 10]*

Kebocoran data yang terjadi pada Tokopedia menunjukkan bahwa perusahaan harus segera melakukan beberapa langkah untuk meningkatkan keamanan data. Kebocoran data ini disebabkan oleh kelemahan dalam sistem keamanan data perusahaan. Kebocoran data ini tidak hanya mempengaruhi kepercayaan pelanggan, tetapi juga dapat menyebabkan kerugian finansial yang signifikan.

Oleh karena itu, Tokopedia harus mengambil beberapa langkah strategis untuk meningkatkan keamanan data dan mencegah kebocoran data serupa di masa depan. Langkah-langkah strategis yang harus dilakukan perusahaan antara lain: mengimplementasikan autentikasi dua faktor untuk meningkatkan keamanan akun pengguna, menggunakan enkripsi data untuk memastikan kerahasiaan data pengguna, memperbarui sistem keamanan secara teratur, dan meningkatkan kesadaran keamanan di kalangan karyawan dan pengguna. Dengan demikian, Tokopedia dapat melindungi data penggunanya dengan lebih baik dan mempertahankan kepercayaan pelanggan.