

**MAKALAH**  
**Membangun Keamanan Bisnis Online**  
**“AKSESORIS”**  
*Ma’Sesori*

Disusun Untuk Memenuhi Tugas Mata Kuliah *e-commerce*



Disusun oleh:  
Christina Febiola Sinaga  
2113025015

**PROGRAM STUDI PENDIDIKAN TEKNOLOGI INFORMASI**  
**FAKULTAS KEGURUAN DAN ILMU PENDIDIKAN**  
**UNIVERSITAS LAMPUNG**  
**2023**

# **BAB I**

## **PENDAHULUAN**

Dalam konteks globalisasi yang terus berlanjut, bisnis online telah menjadi pijakan utama dalam perekonomian modern. Perkembangan teknologi telah memungkinkan terciptanya ekosistem digital yang memfasilitasi transaksi bisnis tanpa batas wilayah. Namun, seiring dengan kemajuan ini, terdapat dampak yang tak terelakkan: ancaman keamanan yang semakin kompleks. Serangan siber, seperti hacking, pencurian identitas, dan serangan malware, telah menjadi ancaman yang mengintai bisnis online. Tidak hanya merugikan secara finansial, tetapi juga dapat merusak reputasi bisnis dan kepercayaan pelanggan. Oleh karena itu, kebutuhan akan sistem keamanan yang tangguh dan inovatif menjadi sangat penting bagi kelangsungan bisnis online dalam menghadapi tantangan ini.

Dalam pandangan ini, kesadaran akan pentingnya keamanan dalam konteks bisnis online menjadi semakin mendesak. Keberadaan ancaman siber yang terus berkembang membutuhkan respons yang cepat dan proaktif dari para pelaku bisnis. Sebuah aspek yang tak terelakkan adalah perlunya investasi tidak hanya dalam infrastruktur teknologi yang handal, tetapi juga dalam sumber daya manusia. Pelatihan dan pemahaman yang lebih baik terhadap keamanan cyber perlu ditanamkan dalam setiap tingkatan organisasi untuk mengurangi risiko serta mengantisipasi kemungkinan serangan yang dapat mengancam bisnis.

Adapun konsekuensi dari kurangnya fokus pada keamanan bisnis online dapat sangat merugikan. Selain kerugian finansial akibat pencurian data dan biaya pemulihan sistem yang terkena serangan, reputasi bisnis juga berisiko rusak. Kehilangan kepercayaan dari pelanggan karena kebocoran informasi pribadi dapat mempengaruhi loyalitas dan mengurangi basis pelanggan. Oleh karena itu, upaya pencegahan dan perlindungan terhadap bisnis online harus menjadi prioritas utama bagi setiap entitas bisnis.

Dalam hal ini, untuk membangun keamanan bisnis online yang kokoh, perlu dilakukan langkah-langkah strategis. Hal ini melibatkan penerapan teknologi keamanan yang canggih, pemantauan sistem secara berkala, serta sosialisasi dan pelatihan kepada setiap individu yang terlibat dalam operasi bisnis online. Dengan demikian, bisnis online dapat membangun fondasi yang tangguh untuk melindungi diri dari ancaman siber yang terus berkembang.

## **BAB II**

### **PEMBAHASAN**

Keamanan bisnis online penting karena memiliki beberapa manfaat, yaitu:

1. Menjaga keamanan data pelanggan.

Data pelanggan merupakan aset penting bagi bisnis online. Data tersebut dapat digunakan untuk berbagai keperluan, seperti pengiriman barang, penagihan, dan pemasaran. Oleh karena itu, penting bagi bisnis online untuk melindungi data pelanggan dari penyalahgunaan.

2. Mencegah penipuan.

Penipuan merupakan salah satu ancaman yang paling umum bagi bisnis online. Penipuan dapat dilakukan dengan berbagai cara, seperti menyamar sebagai pelanggan, menggunakan kartu kredit palsu, atau mencuri data akun. Bisnis online perlu menerapkan langkah-langkah keamanan untuk mencegah terjadinya penipuan.

3. Menjaga reputasi bisnis.

Serangan keamanan yang terjadi pada bisnis online dapat merusak reputasi bisnis tersebut. Pelanggan akan enggan untuk melakukan transaksi dengan bisnis yang tidak memiliki keamanan yang memadai. Oleh karena itu, penting bagi bisnis online untuk menjaga keamanannya untuk melindungi reputasinya.

Ada beberapa langkah yang dapat dilakukan untuk membangun keamanan bisnis online, yaitu:

1. Melakukan audit keamanan.

Langkah pertama yang perlu dilakukan adalah melakukan audit keamanan untuk mengetahui risiko-risiko keamanan yang dihadapi oleh bisnis online. Audit keamanan dapat dilakukan oleh pihak internal atau pihak eksternal yang kompeten.

2. Mengembangkan kebijakan keamanan.

Setelah mengetahui risiko-risiko keamanan, bisnis online perlu mengembangkan kebijakan keamanan yang sesuai. Kebijakan keamanan tersebut harus mencakup hal-hal seperti:

- Keamanan data pelanggan
- Pencegahan penipuan
- Penanganan insiden keamanan

3. Implementasi kebijakan keamanan.

Kebijakan keamanan yang telah dikembangkan perlu diimplementasikan secara konsisten. Bisnis online perlu menyediakan sumber daya yang memadai untuk mendukung implementasi kebijakan keamanan tersebut.

4. Melakukan pelatihan keamanan.

Karyawan merupakan salah satu faktor terpenting dalam keamanan bisnis online. Karyawan perlu dilatih tentang keamanan online untuk meningkatkan kesadaran mereka akan pentingnya keamanan.

## **BAB III**

### **PENUTUP**

#### **1. Kesimpulan**

Keamanan merupakan salah satu aspek penting dalam menjalankan bisnis online. Bisnis online yang tidak memiliki keamanan yang memadai akan rentan terhadap berbagai serangan, seperti pencurian data pelanggan, penipuan, dan malware. Oleh karena itu, penting bagi bisnis online untuk membangun keamanan yang kuat dan terpercaya.

#### **2. Saran**

Bisnis online perlu memperhatikan hal-hal berikut untuk membangun keamanan yang kuat:

- 1) Gunakan teknologi keamanan yang tepat. Ada berbagai teknologi keamanan yang tersedia, seperti firewall, antivirus, dan intrusion detection system. Bisnis online perlu memilih teknologi keamanan yang sesuai dengan kebutuhannya.
- 2) Perbarui perangkat lunak secara berkala. Perangkat lunak yang tidak diperbarui rentan terhadap celah keamanan. Oleh karena itu, bisnis online perlu memperbarui perangkat lunak secara berkala untuk menutup celah keamanan tersebut.
- 3) Lakukan pelatihan keamanan secara berkala. Karyawan perlu dilatih tentang keamanan online secara berkala untuk meningkatkan kesadaran mereka akan pentingnya keamanan.