LAPORAN ANALISIS KEJAHATAN SIBER

Identitas Pelapor

Nama :Lailatul Ma firo

NIM :233140700111027

A. Informasi Kasus

• Judul Kasus : Peran Cyber Security Terhadap Keamanan Data Penduduk Negara i Indonesia (studi kasus: Hacker Bjorka)

• Tahun Kejadian : 2022

• Lokasi : Indonesia

• Jenis Serangan : Data Breach(Kebocoran Data)

• Pihak yang Terlibat :
Penyerang : Hacker Bjorka
Korban : Pemerintah Indonesia,Perusahaan telekomunikasi(indihome),komisi pemilihan umum(KPU),serta Masyarakat umum

• Sumber Referensi : Jurnal Bidang Penelitian Informatika, Vol. 1, No. 1, Oktober 2022,CNBC Indonesia (Dewi, 2022), Jurnal lain yang terkait dengan keamanan siber di Indonesia

B. Analisis Penyebab Insiden

1. Faktor Teknis

- **Kurangnya Enkripsi dan Keamanan Data**

  Data-data penting seperti informasi registrasi SIM Card, data pelanggan Indihome, dan data KPU seharusnya dienkripsi dengan standar keamanan yang tinggi agar tidak mudah diakses oleh pihak yang tidak berwenang.

- **Sistem Keamanan yang Lemah**

  Banyak sistem di Indonesia belum memiliki proteksi keamanan siber yang memadai, seperti firewall yang kuat, sistem deteksi intrusi (IDS/IPS), dan mekanisme autentikasi ganda. Hal ini membuat data lebih rentan terhadap pencurian.

- **Kurangnya Pemantauan dan Respons Cepat**

  Serangan Bjorka terjadi selama beberapa bulan sebelum akhirnya mendapat perhatian serius. Keterlambatan dalam mendeteksi kebocoran data menunjukkan kurangnya sistem pemantauan keamanan siber yang efektif.

2. Faktor Manusia

- **Kurangnya Kesadaran Keamanan Siber**

  Banyak individu dan organisasi yang masih kurang memahami pentingnya keamanan data. Misalnya, penggunaan kata sandi yang lemah dan kebiasaan berbagi informasi sensitif tanpa perlindungan.

- **Pengelolaan Data yang Buruk**

  Data pelanggan dan data pemerintahan seharusnya disimpan dengan protokol keamanan yang ketat. Namun, dalam kasus ini, banyak data tampaknya dapat diakses atau dicuri dengan relatif mudah.

- **Potensi Kebocoran dari Orang Dalam (Insider Threats)**

  Dalam beberapa kasus, kebocoran data bisa berasal dari karyawan yang memiliki akses terhadap informasi sensitif tetapi tidak dijaga dengan baik, atau bahkan dengan sengaja membocorkannya.

3. Faktor Prosedural

- **Tidak Ada Regulasi yang Kuat untuk Perlindungan Data**
  Kurangnya standar dan regulasi yang ketat dalam pengelolaan data di Indonesia menyebabkan banyaknya celah keamanan. Seharusnya ada kebijakan yang mewajibkan enkripsi data serta audit keamanan secara berkala.

- **Minimnya Koordinasi antar Lembaga**
  Pemerintah dan perusahaan telekomunikasi tidak memiliki sistem koordinasi yang kuat untuk menangani kebocoran data secara cepat. Hal ini terlihat dari lambatnya respons terhadap insiden Bjorka.
- Kurangnya Inspeksi Keamanan Berkala
  Organisasi yang menyimpan data sensitif harus rutin melakukan pengujian keamanan (penetration testing) untuk menemukan celah sebelum dieksploitasi oleh peretas. Namun, dalam kasus ini, tampaknya inspeksi semacam itu tidak dilakukan secara efektif.

C. Analisis Risiko

No	Risiko	Probability	Impact	Skor Risiko (P x I)
1	Kebocoran Data pribadi penduduk Indonesia	High	High	9
2	Penyalahgunaan data untuk kejahatan siber(penipuan,phishing)	High	High	9
3	Hilangnya kepercayaan Masyarakat terhadap keamanan data pemerintah	Medium	High	6

D. Analisis Dampak terhadap Perusahaan

1. Dampak Finansial

- Peretasan dan kebocoran data bisa menyebabkan kerugian finansial besar bagi perusahaan yang terdampak, seperti Indihome dan lembaga pemerintah.
- Biaya pemulihan sistem keamanan, investigasi forensik digital, dan kompensasi bagi pelanggan yang terkena dampak bisa mencapai miliaran rupiah.
- Kemungkinan adanya tuntutan hukum atau denda akibat kelalaian dalam melindungi data pelanggan juga bisa meningkatkan beban finansial.

2. Dampak Operasional

- Serangan siber dapat mengganggu operasional perusahaan, terutama dalam pengelolaan data pelanggan dan layanan digital.
- Perusahaan harus mengalokasikan sumber daya untuk memperbaiki sistem yang diretas, yang dapat menyebabkan keterlambatan dalam layanan.
- Adanya kebocoran data juga bisa menghambat proses bisnis, terutama bagi perusahaan yang mengandalkan sistem online dan cloud computing.

3. Dampak Reputasi

- Kepercayaan pelanggan terhadap perusahaan atau instansi yang mengalami kebocoran data bisa menurun drastis.
- Pelanggan mungkin akan berpindah ke layanan lain yang dianggap lebih aman.
- Reputasi pemerintah sebagai pengelola data nasional juga bisa terdampak, menimbulkan keresahan publik dan menurunkan kepercayaan masyarakat terhadap sistem keamanan negara.

4. Dampak Regulasi dan Hukum

- Perusahaan yang mengalami kebocoran data dapat menghadapi tuntutan hukum dari pelanggan atau regulator karena gagal melindungi data pribadi.
- Dalam kasus Indonesia, insiden ini mendorong percepatan implementasi Undang-Undang Perlindungan Data Pribadi (UU PDP) yang mengharuskan perusahaan memperketat kebijakan keamanan data.
- Jika terbukti lalai, perusahaan atau instansi pemerintah bisa dikenakan denda atau sanksi administratif sesuai regulasi yang berlaku.

E. Rekomendasi dan Mitigasi

No	Tindakan Pencegahan	Prioritas	Teknologi/Pendekatan
1	Meningkatkan Sistem Keamanan Siber dengan firewall,enkripsi,dan deteksi intrusi	Tinggi	Implementasi firewall tingkat lanjut, enkripsi AES-256, dan sistem deteksi intrusi (IDS/IPS)
2	Menerakan Autentikasi Multi factor(MFA) untuk mengamankan akses data sensitif	Tinggi	Penggunaan 2FA/MFA pada login akun pegawai dan sistem penting
3	Beckup Data Secara Rutin untuk menghindari kehilangan data akibat serangan	Sedang	Automated cloud backup dengan enkripsi untuk pemulihan cepat pasca insiden

F. Kesimpulan

- Ringkasan utama dari temuan laporan

Keamanan siber memiliki peran yang sangat penting dalam melindungi informasi dari ancaman di dunia digital. Keamanan ini mencakup perlindungan data di media penyimpanan, pengamanan transmisi data, serta perlindungan terhadap infrastruktur digital dari ancaman siber. Dalam konteks pemerintahan, keamanan fakta menjadi salah satu tantangan utama dalam implementasi e-government, khususnya dalam aspek kerahasiaan, integritas, dan ketersediaan informasi.

Badan Siber dan Sandi Negara (BSSN) memiliki peran strategis dalam memastikan keamanan nasional di ruang siber, mendukung pertumbuhan ekonomi digital, dan mengawasi implementasi kebijakan keamanan siber. Situasi ancaman siber yang terus berkembang menjadikan Indonesia sebagai target utama serangan siber, mengingat kekayaan sumber daya alam dan potensinya di bidang ekonomi digital. Oleh karena itu, penguatan kebijakan keamanan siber menjadi keharusan bagi negara maupun sektor bisnis.

- Langkah strategis yang harus dilakukan perusahaan.

1. Penguatan Infrastruktur Keamanan Siber
- Mengimplementasikan enkripsi data untuk melindungi informasi sensitive.
- Meningkatkan keamanan jaringan dengan firewall, sistem deteksi intrusi, dan proteksi terhadap malware.

2. Peningkatan Kesadaran dan Pelatihan Keamanan Siber
- Melatih karyawan dalam mengenali ancaman siber seperti phishing, ransomware, dan social engineering.
- Menerapkan kebijakan keamanan yang ketat, termasuk manajemen akses dan autentikasi berlapis (multi-factor authentication).

3. Penerapan Kebijakan Keamanan yang Ketat
- Mengadopsi standar keamanan seperti ISO 27001 atau framework keamanan siber lainnya.
- Melakukan audit keamanan secara berkala untuk mengidentifikasi dan menutup celah keamanan.
4. Kolaborasi dengan Pihak Berwenang dan BSSN
- Berkoordinasi dengan BSSN dan lembaga terkait untuk berbagi informasi ancaman dan praktik terbaik dalam menangani serangan siber.
- Mengikuti regulasi keamanan siber yang berlaku untuk memastikan kepatuhan dan mitigasi risiko hukum.
5. Pengembangan Teknologi Keamanan Berbasis AI dan Big Data
- Memanfaatkan kecerdasan buatan (AI) untuk mendeteksi ancaman siber lebih dini.
- Menggunakan big data analytics untuk memantau aktivitas yang mencurigakan di sistem perusahaan.