TUGAS MATA KULIAH ETIKA PROFESI

Dosen Pengampu INDRA YUSTIANA, ST., M.Kom

Disusun Oleh :

Faisal Abdul Aziz (20220040130)

TI 22 H

PROGRAM STUDI TEKNIK INFORMATIKA

UNIVERSITAS NUSA PUTRA

Jl. Raya Cibatu Cisaat No.21, Cibolang Kaler. Kec. Cisaat, Telpon (0266)210594 Website : http://nusaputra.ac.id/

TUGAS SESI 3!

Soal Esai Tipe Analisis - Studi Kasus

Kasus: Sebuah perusahaan teknologi besar telah menjadi korban serangan ransomware yang berhasil mengenkripsi seluruh data kritis perusahaan, termasuk data pelanggan dan informasi finansial. Para peretas meminta uang tebusan dalam bentuk cryptocurrency untuk memberikan kunci dekripsi. Sistem backup perusahaan ternyata juga telah terkena dampak serangan ini, sehingga perusahaan tidak dapat segera memulihkan data mereka. Serangan ini menyebabkan operasi bisnis terganggu, dan perusahaan mengalami kerugian finansial yang signifikan serta ancaman kehilangan kepercayaan dari pelanggan.

Pertanyaan:

1. Analisislah jenis ancaman yang dihadapi perusahaan dalam kasus ini dan jelaskan bagaimana serangan ransomware bekerja.
2. Berdasarkan konsep Confidentiality, Integrity, Availability (CIA Triad), jelaskan dampak serangan tersebut terhadap keamanan informasi perusahaan.
3. Sebagai seorang profesional TI, tindakan apa yang seharusnya dilakukan oleh perusahaan untuk mencegah serangan seperti ini di masa depan? Berikan rekomendasi terkait mitigasi
4. risiko dan pemulihan bencana (disaster recovery). Jelaskan langkah-langkah etis yang harus diambil oleh perusahaan terkait dengan privasi dan keamanan data pelanggan yang telah terekspos akibat serangan ini.

Petunjuk Jawaban:

- Jawab dengan menganalisis ransomware sebagai ancaman terhadap availability data.
- Jelaskan bagaimana serangan dapat merusak aspek confidentiality dan integrity.
- Rekomendasikan penggunaan enkripsi, sistem backup terisolasi, patching perangkat lunak,

- dan pelatihan karyawan sebagai mitigasi.
- Diskusikan pentingnya transparansi kepada pelanggan dan kepatuhan terhadap peraturan
- privasi data, seperti GDPR atau undang-undang setempat.

JAWABAN:

Analisis ancaman yang dihadapi perusahaan dan cara kerja serangan ransomware:

Ancaman yang dihadapi perusahaan dalam kasus ini adalah serangan ransomware, yang merupakan bentuk malware yang mengenkripsi data korban sehingga tidak dapat diakses kecuali korban membayar uang tebusan untuk mendapatkan kunci dekripsi. Dalam kasus ini, ransomware berhasil mengenkripsi data kritis perusahaan, termasuk data pelanggan dan informasi finansial.

1. **Cara kerja serangan ransomware:**

- Infeksi awal: Ransomware dapat menyebar melalui email phishing, lampiran berbahaya, atau kerentanan perangkat lunak yang tidak di-patch.
- Enkripsi data: Setelah berhasil masuk ke sistem, ransomware mengenkripsi data pada perangkat yang terinfeksi. Dalam kasus ini, ransomware juga menyerang sistem backup, yang berarti perusahaan tidak bisa memulihkan data dari backup.
- Permintaan tebusan: Setelah enkripsi selesai, ransomware akan menampilkan pesan kepada korban yang berisi instruksi pembayaran dalam cryptocurrency untuk mendapatkan kunci dekripsi.
- Potensi eskalasi: Selain mengenkripsi data, beberapa serangan ransomware modern juga mencuri data korban, meningkatkan risiko kebocoran informasi pribadi atau bisnis.

2. **Dampak serangan terhadap keamanan informasi perusahaan berdasarkan CIA Triad:**

- Confidentiality (Kerahasiaan): Data pelanggan dan informasi finansial yang terenkripsi dapat terekspos jika peretas mencuri dan mengancam untuk membocorkannya. Ini

melanggar kerahasiaan, karena data yang seharusnya hanya diakses oleh pihak yang berwenang dapat diakses oleh pihak tidak berwenang.

- Integrity (Integritas): Serangan ransomware dapat memengaruhi integritas data, karena meskipun perusahaan mendapatkan kunci dekripsi, tidak ada jaminan bahwa data yang dipulihkan tidak rusak atau diubah. Bahkan, ransomware dapat memodifikasi, menghapus, atau merusak data selama proses enkripsi.

- Availability (Ketersediaan): Serangan ransomware secara langsung mengancam ketersediaan data karena data yang dienkripsi tidak dapat diakses oleh perusahaan. Sistem backup yang juga terkena ransomware memperburuk situasi, membuat perusahaan tidak mampu segera memulihkan operasional bisnisnya.

3. Tindakan yang seharusnya dilakukan untuk mencegah serangan dan rekomendasi mitigasi risiko:

- Untuk mencegah serangan ransomware di masa depan, perusahaan perlu mengadopsi pendekatan berlapis terhadap keamanan informasi. Berikut rekomendasi terkait mitigasi risiko dan pemulihan bencana:

- Backup yang terisolasi dan terenkripsi: Perusahaan harus memiliki sistem backup yang terpisah dari jaringan utama (offline atau berbasis cloud yang aman) dan terenkripsi. Ini akan memastikan bahwa meskipun ransomware menyerang sistem utama, backup tetap utuh dan dapat dipulihkan.

- Patching dan pembaruan sistem: Kerentanan perangkat lunak yang tidak di-patch sering menjadi jalan masuk bagi ransomware. Perusahaan harus secara rutin memperbarui perangkat lunak dan sistem operasi untuk menutup celah keamanan.

- Penggunaan enkripsi yang kuat: Data sensitif perusahaan harus selalu dienkripsi, baik saat disimpan maupun saat dikirim. Ini akan melindungi data meskipun terjadi kebocoran.

- Pelatihan karyawan: Serangan phishing sering kali menjadi metode awal infeksi ransomware. Perusahaan harus memberikan pelatihan keamanan siber secara rutin

kepada karyawan agar mereka dapat mengenali tanda-tanda phishing dan ancaman keamanan lainnya.

- Pemantauan dan deteksi dini: Mengimplementasikan solusi pemantauan keamanan seperti SIEM (Security Information and Event Management) untuk mendeteksi aktivitas mencurigakan lebih awal, serta melakukan analisis forensik jika ada pelanggaran.

- Disaster recovery plan (DRP): Memiliki rencana pemulihan bencana yang diuji secara berkala untuk memastikan bisnis dapat pulih dengan cepat setelah insiden, termasuk pemulihan data, pemulihan sistem kritis, dan prosedur komunikasi darurat.

4. Langkah-langkah etis terkait privasi dan keamanan data pelanggan yang terekspos:

- Transparansi kepada pelanggan: Perusahaan harus segera memberi tahu pelanggan tentang pelanggaran data. Komunikasi yang jelas dan tepat waktu akan membantu menjaga kepercayaan pelanggan, meskipun data mereka telah terekspos. Informasi yang diberikan harus mencakup jenis data yang terekspos, risiko yang mungkin dihadapi pelanggan, serta langkah-langkah yang diambil perusahaan untuk mengatasi masalah ini.

- Perlindungan data lanjutan: Perusahaan harus memberikan panduan kepada pelanggan tentang tindakan yang dapat mereka ambil untuk melindungi diri, seperti mengubah kata sandi, waspada terhadap upaya phishing, dan memantau aktivitas keuangan mereka.

- Kepatuhan terhadap regulasi privasi: Perusahaan harus memastikan bahwa mereka mematuhi peraturan privasi yang berlaku, seperti GDPR di Eropa atau undang-undang lokal lainnya. Ini termasuk melaporkan pelanggaran data kepada otoritas yang berwenang dalam batas waktu yang ditetapkan.

- Langkah kompensasi: Jika pelanggaran data menyebabkan kerugian bagi pelanggan, perusahaan harus mempertimbangkan kompensasi yang sesuai, seperti menyediakan layanan pemantauan kredit gratis atau perlindungan identitas bagi pelanggan yang terdampak.

Dengan mengikuti langkah-langkah ini, perusahaan tidak hanya dapat memitigasi risiko di masa depan tetapi juga mengurangi dampak dari insiden keamanan ini dan menjaga kepercayaan pelanggan serta reputasinya