Prinsip - Prinsip Sistem Informasi

Studi Kasus 1

Kelompok C20:

1. Yosef Nuraga Wicaksana 2206082751
2. Clement Samuel Marly 2206082114
3. Alexander Audric Johansyah 2206815466
4. Tohodo Betrand Simamora 2206083376

1. Jika universitas membayar uang tebusan, seberapa besar kemungkinan data akan dipulihkan oleh penyerang?

Tidak ada cara yang tepat atau pasti untuk memperhitungkan seberapa besar kemungkinan data akan dipulihkan oleh penyerang dengan membayar uang tebusan kepada penyerang. Terdapat kemungkinan bahwa penyerang tidak memberikan kunci akses untuk memulihkan data yang terenkripsi ataupun penyerang menuntut uang tebusan yang lebih banyak.

2. Pilihan lain apa yang dimiliki universitas untuk memulihkan data tersebut?

Langkah alternatif yang dapat dilakukan universitas dalam memulihkan data yang telah dienkripsi oleh serangan ransomware adalah dengan memulihkan data melalui *backup* atau cadangan data apabila pihak universitas memiliki *backup* atau cadangan data. Langkah lain yang dapat dilakukan adalah memecah enkripsi serangan ransomware dari pihak penyerang sehingga pihak universitas dapat kembali memiliki akses ke data tersebut. Universitas juga bisa melaporkan permasalahan ini ke pihak kepolisian dan mencari lokasi penyerang untuk mendapatkan kunci enkripsi.

3. Buatlah skenario jika universitas disarankan untuk membayar uang tebusan.

Universitas tidak memiliki *backup* atau cadangan data dan enkripsi yang digunakan oleh penyerang tidak bisa ditembus oleh tim emergensi atau IT universitas.

- Skenario terbaik setelah membayar uang tebusan

Universitas membayar uang tebusan dan kunci akses diberikan oleh penyerang kepada pihak universitas. Universitas bisa mengakses kembali semua data yang telah terenkripsi oleh penyerang.

- Skenario terburuk setelah membayar uang tebusan

  Universitas membayar uang tebusan, tetapi kunci akses tidak diberikan oleh penyerang sehingga data-data universitas tidak bisa diakses. Penyerang meminta bayaran lebih untuk memberikan kunci akses data-data yang terenkripsi dan tidak berencana untuk memberikan kunci enkripsi sama sekali. Universitas menanggung semua resiko dari hilangnya data catatan akademik mahasiswa, informasi keuangan, informasi personel fakultas dan administrasi, dan catatan gaji.

4. Bagaimana rekomendasi Anda kepada universitas dalam menanggapi permintaan dari penyerang? Mengapa?

Dalam memberikan rekomendasi, diperlukan beberapa analisis dalam menanggapi penyerangan *cyber* agar pihak universitas dapat menentukan keputusan yang paling tepat dan meminimalisir kerusakan yang perlu ditanggung. Berikut adalah langkah-langkah dalam menanggapi permintaan dari penyerang.

1. Analisis Situasi

   Analisis situasi perlu dilakukan oleh pihak universitas sebagai langkah paling dasar dalam mengembangkan susunan skema dalam menanggapi serangan *cyber* dalam data. Dalam tahap ini beberapa hal yang perlu dianalisis adalah:

   a. Analisis kredibilitas penyerangan dimana universitas perlu memastikan apakah penyerang benar-benar memiliki akses dan kontrol pada data universitas. Hal ini perlu dilakukan agar terhindar dari tipuan penipu untuk mendapatkan uang tebusan.
   b. Analisis seberapa besar resiko data yang dimiliki universitas dan para *stakeholders* dalam beberapa aspek seperti aspek keselamatan dan finansial para *stakeholder*.

2. Pertimbangan alternatif

   Pertimbangan alternatif perlu dilakukan untuk mengetahui apakah terdapat cara lain memulihkan data selain membayar uang tebusan kepada penyerang seperti memulihkan data melalui *backup data,* dekripsi data yang telah terenkripsi oleh *ransomware*, dan bekerja sama dengan pihak kepolisian. Langkah alternatif kemudian di pertimbangkan dengan alternatif-alternatif lain dan dipilih langkah yang memiliki resiko terkecil. Apabila langkah alternatif dapat dilakukan maka pembayaran uang tebusan dapat dihindari sehingga meminimalisir kerusakan yang ditanggung.

Melihat dari kasus yang terjadi pada penyerangan dimana kredibilitas penyerangan asli dan resiko data yang besar karena data catatan akademik mahasiswa, informasi keuangan, informasi personel fakultas dan administrasi, serta catatan gaji di universitas dapat dikategorikan sebagai data vital universitas. Maka dari itu, terdapat beberapa saran kepada Universitas untuk menanggapi permintaan penyerang.

1. Apabila langkah alternatif seperti memulihkan data dengan *backup* data, deskripsi data dapat dilakukan kurang dari waktu maksimal ransomware yakni dua hari, maka pihak universitas dapat memulihkan data tersebut tanpa membayar uang tebusan. Strategi ini dapat dipakai karena data yang diserang dapat diakses kembali oleh universitas tanpa membayar uang tebusan dalam kurang dari dua hari dengan restorasi menggunakan *backup* / cadangan data atau dekripsi data yang terkena *ransomware*.

2. Apabila tidak ada satupun langkah alternatif yang dapat dilakukan untuk memulihkan data, maka universitas perlu melapor ke pihak kepolisian dan membayar uang tebusan. Universitas juga perlu secara terstruktur dengan memonitor pengembalian data untuk mengurangi resiko kerusakan yang lebih besar. Strategi ini hanya dilakukan apabila tidak ada jalan lain selain membayar uang tebusan karena memiliki kemungkinan skenario terburuk, yaitu penyerang tidak berencana memberikan kunci akses dan meminta bayaran lebih setelah diberikan uang tebusan.

Referensi

Janacek, B. (2022, November 9). *Is Encryption Enough to Protect Yourself?* DataMotion. https://datamotion.com/is_encryption_enough_to_protect_yourself/#:~:text=Most%20software%20. Diakses 12 Februari 2023.

Jahankhani, H. (n.d.). *Strategy, Leadership, and AI in the Cyber Ecosystem: The Role of Digital Societies in Information Governance and Decision Making*. Diakses 12 Februari 2023.