Download Gaido Mobile

Ekonomi Syariah

IT SUPPORT
GAIDO BANK SYARIAH

2023

Materi

Pengenalan Virus Ransomware Bahayanya Bagi Perbankan dan Pencegahan Dini Terkena Virus Ransomware

BAB 1. PENDAHULUAN

1.1 Latar Belakang

Pada hari senin, tanggal 8 Mei 2023 sejumlah nasabah Bank Syariah Indonesia (BSI) mengeluhkan mereka tidak bisa mengakses aplikasi BSI Mobile. Masalah tersebut muncul dengan *notifikas*i yang menyebutkan permintaan transaksi nasabah tidak bisa diproses.

Pihak Bank Syariah Indonesia (BSI) memberikan pernyataan error tersebut dikarenakan BSI tengah melakukan *maintenance system.* Oleh karena itu layanan BSI saat hari itu tidak bisa digunakan dengan normal dan akan segera normal secepatnya.

Setelah beberapa hari layanan BSI tidak kunjung normal banyak orang menduga bahwa *Core Banking System* BSI terkena serangan virus Ransomware yang akan kita bahas oleh pihak yang tidak bertanggung jawab.

Isu atau dugaan tersebut diperkuat oleh postingan Twitter oleh akun @draktracer_int pada hari sabtu, 13 Mei 2023 yang menyatakan bahwa BSI telah terkena sorangan Ransomware oleh organisasi yang bernama LockBit 3.0 mereka mengaku telah mencuri 15 Juta catatan nasabah, informasi karyawan, dan sekita 1.5 terabyte data internal.

Data-data tersebut akan dipublikasikan disitus *Darkweb* untuk di jual jika Bank Syariah Indonesia tidak memenuhi permintaan yang diajukan oleh pihak LockBit 3.0.

1.2 Tujuan

Sebagaimana dijelasakan pada latar belakang bahwa bahaya serangan ransomware bagi perusahaan sangat merugikan terutama bagi layanan jasa keuangan perbankan khususnya Gaido Bank Syariah karena ada unsur kepercayaan nasabah yang harus dijaga atas privasi data mereka dan keamanan uang mereka yang disimpan di Gaido Bank Syariah.

Oleh karena itu, artikel ini bertujuan untuk mengedukasi karyawan Gaido Bank Syariah khususnya mengenal tentang apa itu virus ransomware, bahaya yang ditimbulkan bagi perusahaan dan data perusahaan jika terkena ransomware serta cara pencegahan dini yang bisa dilakukan oleh karyawan agar terhindar dari serangan virus ransomware.

Upaya ini dilakukan agar nasabah Gaido Bank Syariah dapat percaya bahwa data dan saldo mereka akan aman dalam database Gaido Bank Syariah karena karyawan dan seluruh elemen yang terlibat dalam proses bisnis Gaido Bank Syariah peduli terhadap serangan virus khususnya ransomware.

BAB 2. PENGENALAN VIRUS RANSOMWARE, BAHAYANYA BAGI PERBANKAN DAN PENCEGAHAN DINI TERKENA VIRUS RANSOMWARE

2.1 Apa itu Ransomware ?

Ransomware adalah salah satu jenis *malware* (*malicious software*) yang bekerja dengan metode enkripsi—mengolah data menjadi kode yang tidak dapat dibaca oleh perangkat. Sehingga, menyebabkan korban tidak dapat mengakses perangkatnya sebelum data tersebut didekripsi—diolah kembali dari bentuk yang sudah dienkripsi agar dapat dibaca oleh perangkat.

Untuk dapat mendekripsi data pada perangkat yang terinfeksi Ransomware, kamu memerlukan kode dekripsi yang akan ditawarkan oleh peretas dengan membayar tebusan. Jika dalam waktu tertentu kamu belum dapat mendekripsikan perangkatmu, maka data-data yang ada di perangkat akan hilang.

Dari semua jenis *malware* yang ada, Ransomware adalah salah satu yang paling berbahaya. Berbeda dengan *malware* lainnya, Ransomware dapat mengacaukan sistem perangkat hingga tidak dapat dioperasikan.

Selain itu, Ransomware juga memiliki sifat yang dapat menyebar dan menginfeksi perangkat di sekitarnya. Sehingga, sangat berbahaya jika tidak segera ditangani dengan cepat.

Berikut ini statistik perkembangan Ransomware beberapa tahun terakhir berdasarkan situs web *cyber security* PurpleSec:

- Tebusan Ransomware rata-rata pada tahun 2021 meningkat sebesar 82% dari tahun ke tahun, menjadi $570.000 atau setara dengan 8,1 miliar rupiah.
- Sebanyak 121 serangan Ransomware dilaporkan pada Q1 2021, meningkat 64% dari tahun ke tahun.
- Ransomware terbukti meningkat dengan salah satu jenis Ransomware, Ryuk, yang mengalami peningkatan pesat sebesar 543% selama Q4 2018.
- Pada 2019, Ransomware dengan cara *phising* meningkat sebesar 109%, dengan varian Ransomware baru tumbuh sebesar 46%.
- Serangan Ransomware meningkat 41% pada tahun 2019 dengan 205.000 bisnis kehilangan akses data mereka.
- Ransomware telah menjadi bentuk serangan siber yang populer dalam beberapa tahun terakhir, tumbuh sebesar 350% pada 2018.

2.1.1 Cara Kerja Ransomware

Umumnya, ada tujuh tahap bagaimana Ransomware bekerja untuk mengacaukan sistem di perangkatmu. Berikut penjelasannya:

1. Infeksi

Ransomware yang terunduh secara tidak sengaja mulai meng-*install* secara diam-diam di perangkatmu.

2. Eksekusi

Setelah ter-*install*, Ransomware mulai memindai dan memetakan lokasi *file* yang akan menjadi targetnya. *Malware* ini dapat menargetkan *file* yang disimpan di penyimpanan lokal maupun penyimpanan awan (*cloud*). Bahkan, beberapa jenis Ransomware dapat menghapus atau mengenkripsi *file* maupun folder *backup*.

3. Enkripsi

Di tahap ini, Ransomware mulai bekerja dengan melakukan pertukaran kunci dengan Command and Control Server, menggunakan kunci enkripsi untuk mengacak semua *file* yang ditemukan di tahap Eksekusi. *Malware* jenis ini juga mengunci akses ke data di perangkat.

4. Notifikasi

Setelah berhasil mengambil alih data di perangkatmu, Ransomware biasanya akan memunculkan notifikasi pengguna yang berisi informasi tebusan yang harus dibayarkan untuk mendapatkan kode dekripsi.

5. Pembersihan

Setelah berhasil mengenkripsi data yang diinginkan, Ransomware biasanya berhenti dan menghapus dirinya sendiri, dan hanya menyisakan file instruksi pembayaran.

6. Pembayaran

Jika kamu memilih untuk membayar tebusan, kamu akan diminta untuk mengikuti instruksi. Peretas biasanya menggunakan layanan TOR tersembunyi untuk berkomunikasi agar terhindar dari deteksi pemantauan lalu lintas jaringan.

7. Dekripsi

Setelah melakukan pembayaran, korban akan mendapatkan kode dekripsi untuk memulihkan kembali akses ke perangkatnya. Walaupun begitu, membayar tebusan sangat tidak disarankan karena tidak ada jaminan *file* atau folder milikmu akan kembali seperti sedia kala.

2.1.2 Jenis-Jenis Ransomware

Ada beberapa jenis Ransomware yang dibedakan berdasarkan cara kerjanya. Berikut ini dua jenis Ransomware yang paling umum ditemukan:

1. Encrypting Ransomware

Ransomware jenis ini menginfeksi perangkat dengan cara mengenkripsi *file* maupun folder penting yang ada di perangkat korban. Setelah target berhasil terkunci dan terenkripsi, akan muncul notifikasi mengenai tebusan yang harus dibayarkan untuk membuka kembali data yang telah terkunci.

Contoh Encrypting Ransomware:

- WannaCry
- CryptoWall
- CryptoLocker
- Locky

2. Locker Ransomware

Ransomware jenis ini tidak bekerja dengan cara mengenkripsi *file* maupun folder milik korban, melainkan mengunci akses korban ke perangkat. Biasanya, target Locker Ransomware adalah penguncian *file* maupun perangkat. Tapi terkadang, *malware* jenis ini juga menyasar *hardware* milik korban seperti *keyboard* atau *mouse*.

Locker Ransomware termasuk gangguan tingkat rendah yang masih bisa ditangani cukup dengan menghapus *script*, dsb. Sehingga,

tebusan yang dibayarkan untuk *malware* jenis ini bisa dibilang lebih sedikit.

Contoh Locker Ransomware:

- Winlocker
- Reveton

2.2 Bahaya Ransomware Bagi Perbankan

Ada beberapa bahaya yang ditimbulkan setelah sebuah perusahaan khususnya Layanan Jasa Keuangan Perbankan jika terkena oleh serangan virus ransomware.

1. **Core Banking System Lumpuh/Mati**

Setelah terkena serangan ransomware otomatis perusahaan atau Lembaga Jasa Keuangan khususnya Gaido Bank Syariah harus mematikan semua akses yang akan tertuju ke database karena agar virus tidak menyebar lebih jauh dan mengambil atau mengunci data yang lebih banyak dan penting.

2. **Transaksi Akan Terhenti**

Semua transaksi yang dilakukan oleh Gaido Bank Syariah hakikatnya harus tercatat dalam *Core Banking System* karena akan terjunal otomatis dengan neraca dan informasi nasabah lainnya seperti tabungan dan pembiayaan. Tapi karena sedang terjadi pemulihan data pada database *Core Banking System* maka nasabah dan karyawan tidak bisa melakukan transaksi sebelum databasae pulih.

3. **Krisis Kepuasan dan Kepercayaan Nasabah Terhadap Bank**

Jika pemulihan berjalan cukup lama dan nasabah tidak bisa menabung, menarik tabungan dan membayar angsuran pembiayaan nasabah akan merasa kecewa atas pelayanan yang diberikan.

4. Penarikan Masal Saldo / Pindah ke Bank Lain

Dikarenakan nasabah sudah krisis kepercayaan kepada Bank yang terkena ransomware, akhirnya nasabag menarik masal saldonya dan dipindahkann ke bank lain dengan begitu akan terjadi masalah likuditas pada bank tersebut.

5. Reputasi Buruk

Akan sulit bagi sebuah bank yang terkena ransomware dan telah dipublikasikan ke publik untuk mendapatkan kembali kepercayaan nasabahnya.

2.3 Cara Mencegah Serangan Ransomware

Setelah mengetahui apa itu Ransomware, saatnya mempelajari cara mencegah Ransomware agar perangkatmu tetap aman. Berikut ini yang dapat kamu lakukan:

1. Hindari halaman web tanpa HTTPS

HTTPS atau *Hypertext Transfer Protocol Secure* berfungsi untuk mengamankan pertukaran data yang terjadi di internet dengan melakukan enkripsi data. HTTPS menjamin keamanan kamu saat mengunjungi *website* ber-HTTPS melalui 3 aspek: autentikasi, integritas, dan enkripsi.

Mengunjungi *website* yang menggunakan HTTPS akan membantumu terhindar dari serangan *malware* tersembunyi. Kamu bisa mengetahui apakah suatu *website* sudah menggunakan HTTPS dengan mengecek URL *website* tersebut.

2. Hindari file dari situs tidak resmi

Membuka situs yang tidak resmi saja sudah cukup berbahaya, apalagi jika kamu mengunduh dan meng-*install* sesuatu dari situs

tersebut. *File* yang ada pada situs tidak resmi adalah tempat paling nyaman bagi Ransomware untuk bersembunyi dan menunggu korban untuk mengunduhnya.

Oleh karena itu, usahakan selalu mengunduh *file* dari situs resmi yang sudah terjamin keamanannya.

3. Hindari iklan dan tautan mencurigakan

Malvertising atau *malware advertising* adalah metode yang sering digunakan peretas untuk menyebarkan *malware*, termasuk Ransomware. Kamu bisa tanpa sengaja mengeklik suatu tautan iklan, kemudian tanpa disadari Ransomware telah ter-*install* di perangkatmu. Untuk itu, berhati-hatilah jika melihat iklan maupun tautan yang mencurigakan di internet.

4. Backup data secara rutin

Cara kerja Ransomware adalah dengan mengenkripsi data dan mengancam untuk menghapusnya jika korban tidak membayar tebusan. Namun, jika kamu memiliki *backup* data yang baik, tentunya hal tersebut tidak akan menjadi masalah besar. Inilah alasan pentingnya mengapa kamu harus selalu melakukan *backup* data secara rutin.

5. Aktifkan firewall dan antivirus

Firewall dan antivirus adalah cara paling efektif untuk mencegah serangan Ransomware maupun jenis *malware* lainnya. *Firewall* bekerja dengan menyaring data apa saja yang diakses oleh perangkat saat tersambung ke internet.

Firewall juga akan bertindak selayaknya tembok yang melindungi perangkat dari pencurian data oleh peretas. Namun, perlindungan *firewall* saja tidaklah cukup, dan peretas akan selalu mencari celah untuk masuk ke dalam perangkatmu.

Untuk itu, kamu juga harus memasang antivirus untuk memberikan perlindungan ekstra terutama dari *malware* berbahaya seperti Ransomware.

6. Gunakan jaringan yang aman

Bagi kamu yang sering menggunakan WiFi publik, maka harus berhati-hati. Karena tidak semua jaringan WiFi publik dilengkapi dengan keamanan untuk mengenkripsi data yang kamu berikan saat berselancar di internet.

Akibatnya, data milikmu dapat dengan mudah bocor dan diketahui oleh peretas untuk mengirimkan *malware* ke perangkatmu. Kalau tidak ingin hal ini terjadi, usahakan untuk selalu menggunakan jaringan yang aman, ya.

BAB 3. PENUTUP

Dalam artikel ini, kami telah membahas beberapa efek jika sebuah bank terkena ransomware serta aspek terkait ransomware dan cara-cara untuk melindungi dari serangan tersebut. Kami mencakup tiga poin utama yang penting untuk diingat :

1. Kesadaran Keamanan Digital : Penting untuk meningkatkan kesadaran tentang ancaman ransomware dan cara-cara untuk mencegah serangan. Ini melibatkan pendidikan tentang praktik keamanan online yang baik, seperti menghindari membuka lampiran email yang mencurigakan, menghindari mengklik tautan yang tidak dikenal.
2. Backup Data yang Teratur : Melakukan backup data secara teratur adalah langkah penting dalam melindungi diri dari ancaman ransomware. Dengan memiliki salinan cadangan data yang terpisah dari sistem utama Anda, Anda dapat memulihkan file Anda tanpa harus membayar tebusan jika terjadi serangan ransomware. Pastikan untuk menyimpan salinan cadangan di tempat yang aman dan terlindungi.
3. Selalu Menjaga Kepercayaan Nasabah : Memberikan keamanan dan kenyamanan kepada nasabah yang bertransaksi di Gaido Bank Syariah sehingga nasabah akan terus menggunakan layanan dan menyimpan uang mereka secara berkala.

Namun, penting juga untuk diingat bahwa tidak ada metode perlindungan yang sepenuhnya terjamin. Serangan ransomware terus berkembang dan para penjahat siber terus mencari celah dalam keamanan. Oleh karena itu, selalu menjadi kebijaksanaan untuk tetap waspada, mengikuti perkembangan terbaru dalam ancaman keamanan, dan mengambil tindakan proaktif untuk melindungi diri Anda.

Dengan meningkatnya kesadaran dan upaya yang tepat, kita dapat mengurangi risiko dan dampak serangan ransomware. Dalam menghadapi ancaman ini.