Merkurius : Jurnal Riset Sistem Informasi dan Teknik Informatika
Volume. 2 No. 4 Juli 2024
e-ISSN: 3031-8912; p-ISSN: 3031-8904, Hal. 102-109
DOI: https://doi.org/10.61132/merkurius.v2i4.151

Analisis Bahaya Serangan Ransomeware Terhadap Layanan Perbankan

Nurul Monika Larasati
Universitas Malikussaleh
E-mail: nurul.220420020@mhs.unimal.ac.id

Rayyan Firdaus
Universitas Malikussaleh
E-mail: rayyan@unimal.ac.id

Address: Jl. Cot Tengku Nie, Reulet, Muara Batu, Aceh Utara
Corresponding author: nurul.220420020@mhs.unimal.ac.id

Abstract: *In the ever-growing digital era, banking services also continue to develop and become important for both individuals and businesses to carry out financial transactions quickly and easily. With these technological advances, serious concerns have arisen regarding the security of banking service data. Ransomware is a type of malicious program or malware that threatens to destroy or block access to important data or systems until a ransom is paid by the victim. Ransomware can infect computers in various ways, for example through attached files that the victim downloads, or attacking software directly by looking for vulnerable loopholes. Ransomware attacks have caused many losses, especially in the banking sector, both in terms of financial and customer data security. Protection of banking services from cyber attacks is very important. Proactive prevention efforts, early detection, quick response, application of appropriate technology and implementation of strong data security policies are crucial elements in maintaining the integrity and security of financial transactions. Therefore, it is very important for banking services to understand ransomware attacks and the dangers of ransomware by strengthening computer data security. The research method used is descriptive qualitative research using the literature study method.*

Keywords*: Banking Services, Ransomware, data security*

Abstrak: Di era digital yang terus berkembang, layanan perbankan juga terus berkembang dan menjadi penting baik bagi individu maupun bisnis untuk melakukan transaksi keuangan dengan cepat dan mudah. Dengan kemajuan teknologi tersebut, kekhawatiran serius muncul mengenai keamanan data layanan perbankan. Ransomware merupakan jenis program jahat atau malware yang mengancam untuk menghancurkan atau memblokir akses ke data atau sistem penting hingga tebusan dibayarkan oleh korban. Ransomware dapat menginfeksi komputer melalui berbagai cara, misalnya melalui file lampiran yang di download korban, atau menyerang langsung pada software dengan mencari celah yang rentan. Serangan ransomware telah memberikan banyak kerugian khusunya di bidang perbankan baik dari segi finansial maupun segi kemanan data nasabah. Perlindungan terhadap layanan perbankan dari serangan siber menjadi sangat penting. Upaya pencegahan yang proaktif, deteksi dini, respons cepat, penerapan teknologi yang tepat dan penerapan kebijakan keamanan data yang kuat menjadi elemen krusial dalam menjaga integritas dan keamanan transaksi keuangan. Oleh karena itu, sangat penting bagi layanan perbankan untuk memahami serangan ransomware dan bahayanya ransomware dengan melakukan penguatan keamanan data komputer. Metode penelitian yang digunakan adalah penelitian kualitatif deskriftif dengan menggunakan metode studi pustaka.

Kata Kunci: Layanan Perbankan; Ransomware; Keamanan data

Received: Mei 30, 2024; Accepted: Juni 20, 2024; Published: Juli 30, 2024
* Nurul Monika Larasati, nurul.220420020@mhs.unimal.ac.id

PENDAHULUAN

Di era digital yang terus berkembang, layanan perbankan juga terus berkembang dan menjadi penting baik bagi individu maupun bisnis untuk melakukan transaksi keuangan dengan cepat dan mudah. Dengan kemajuan teknologi tersebut, kekhawatiran serius muncul mengenai keamanan data layanan perbankan.

Salah satu serangan siber yang umum dilakukan oleh hacker adalah ransomware, yaitu jenis virus tertentu yang menyebabkan kerusakan pada sistem komputer dan menciptakan risiko keamanan dengan membatasi akses ke data penting sampai data tersebut dibayar tebusannya. Berdasarkan statistik BSSN, sektor keuangan menduduki posisi ketiga, yang paling terkena dampak anomali internet setelah sektor pemerintahan dan energi. Berdasarkan data yang dikumpulkan pada tahun 2023, dari 160 juta kasus malware anomali, sekitar 966.533 teridentifikasi sebagai ransomware. Kondisi ini menekankan betapa pentingnya meningkatkan keamanan sektor keuangan di Indonesia.

Serangan ransomware telah banyak dilaporkan pada layanan perbankan di bank - bank Indonesia. Menurut ptsecurity.com, kerugian yang ditimbulkan oleh lembaga keuangan berjumlah besar kira-kira sekitar $5,9 juta per insiden, lebih besar dari rata - rata di semua industri. Peristiwa ransomware pernah terjadi pada tahun 2023 di PT Bank Syariah Indonesia yang mengakibatkan layanan bank tersebut tidak dapat digunakan selama empat hari. Vaksincom Alfons Tanujaya, pakar forensik digital menyatakan bahwa :

" *PT Bank Syariah Indonesia awalnya mengakatan bahwa pemeliharaan sistem adalah akar penyebab permasalahan pada layanan BSI, namun pekerjaan ini biasanya dilakukan di luar jam kerja reguler atau hari libur. Selain itu, eror tersebut terjadi lebih dari satu hari yang menandakan adanya gangguan yang sangat serius*", dilansir dari kontan.co.id.

Pada Rabu, 11 Maret 2023, Direktur PT Bank Syariah Indonesia akhirnya menyampaikan bahwa adanya dugaan telah terjadi serangan ransomware pada PT Bank Syariah Indonesia.

Serangan ransomware telah memberikan banyak kerugian khususnya di bidang perbankan baik dari segi finansial maupun segi kemanan data nasabah. Oleh karena itu, dibutuhkan pemahaman yang kuat mengenai apa itu ransomware dan bagaimana cara dan upaya untuk menghindarinya.

METODE PENELITIAN

Penelitian ini dilakukan dengan menggunakan metode kualitatif. Penelitian kualitatif adalah penelitian yang bersifat alamiah atau bersetting apa adanya dari fenomena yang terjadi

di lapangan dan makna dari fenomena tersebut yang dapat dijadikan pelajaran untuk mengembangkan konsep teoritis.

Dengan itu, jenis penelitian kualitatif yang digunakan adalah penelitian kualitatif deskriftif dengan menggunakan metode studi pustaka. Studi pustaka adalah metode penelitian yang mengkaji atau mempertimbangkan jurnal-jurnal terkait dengan serangan siber pada layanan perbankan dan cara untuk megatasi serangan siber tersebut. Data dan informasi diperoleh dari jurnal dan artikel ilmiah terkini dalam kurun waktu lima tahun terakhir yang membahas tentang serangan siber pada layanan perbankan.

HASIL DAN PEMBAHASAN

Ransomware adalah program atau malware jahat yang mengancam untuk menghancurkan atau memblokir data atau sistem penting sampai korban membayar tebusan. Meskipun awalnya menyerang individu, serangan ransomware yang dilakukan oleh hacker telah meningkat dan menjadi lebih sulit untuk ditangani dalam beberapa tahun terakhir. Serangan seperti ini dilakukan oleh kelompok pencuri yang menggunakan intelijen yang mereka peroleh untuk meretas jaringan bisnis. Beberapa serangan bahkan sangat rumit sehingga pelaku dapat menggunakan informasi keuangan internal mereka untuk menentukan jumlah tebusan yang diminta.

Ransomware dapat menginfeksi komputer melalui berbagai cara, misalnya melalui file lampiran yang di-download korban, atau menyerang langsung pada software dengan mencari celah yang rentan. Untuk membuka data tersebut, pelaku peretasan biasanya akan meminta sejumlah uang tebusan kepada korban.

Beberapa contoh serangan *ransomware* yang populer antara lain:

- *Encrypting Ransomware* adalah jenis yang sering digunakan. Serangan jenis ini mengenkripsi file korban dengan algoritma enkripsi yang sangat rumit sehingga file korban tidak bisa diakses tanpa adanya kunci deskripsi yang tepat. WannaCry dan CryptoLocker adalah contoh ransomware enkripsi yang terkenal.
- *Locker Ransomware* berbeda dengan *Encrypting Ransomware* karena jenis ini tidak mengenkripsi file, sebaliknya sistem ini memblokir akses ke sistem secara keseluruhan. Pesan yang dikirim oleh locker ransomware biasanya menghalangi orang untuk membuka sistem di dalam komputer mereka. Ransomware ini biasanya berkedok sebagai pemberitahuan palsu dari pihak berwenang seperti polisi dan pihak keamanan.

- *Master Boot Record (MBR) Ransomware* adalah jenis ransomware yang menargetkan perangkat komputer. Jenis ini akan mengubah MBR menjadi kode yang membatasi akses korban ke sistem. Artiny, perangkat tidak dapat diakses hingga tebusan dibayar.
- *Mobile Ransomware* adalah jenis yang dibuat spesifik untuk menargetkan perangkat mobile. Ini menyebabkan data dalam perangkat terenskripsi serta membatasi akses ke sistem dan fungsi penting. Android/Filecoder.C merupakan contohnya.
- *Scareware Ransomware* menggunakan teknik penipuan untuk mengirimkan pesan ancaman palsu kepada korban. Pesan palsu ini berisi peringatan palsu tentang perilaku melanggar hukum atau aktivitas ilegal yang diyakini dilakukan oleh korban, agar korban takut dan memutuskan untuk membayar tebusan.

Cara Kerja Ransomware

Ransomware adalah jenis serangan digital yang sangat berbahaya. Organisasi, perusahaan, bahkan individu bisa jadi targetnya dengan tujuan untuk meminta tebusan. Proses terjadinya serangan ransomware, seperti yang dilaporkan oleh bca.co.id, terdiri dari beberapa langkah sebagai berikut:

1. Perangkat lunak jahat (malware) secara tidak sengaja diunduh oleh korban lewat salah satu media yang digunakan oleh peretas.
2. Setelah terinstal, malware akan mengeksplorasi perangkat untuk menemukan data penting dan berharga yang kemudian digunakan untuk mengancam pemiliknya.
3. Ketika telah menemukan data atau informasi penting, malware akan mengenkripsi file-file dan data-data penting, sehingga pemiliknya tidak dapat mengaksesnya.
4. Peretas akan mengirimkan pesan yang disebut *Ransom Notes* kepada pemilik data yang mengancam akan mengembalikan data mereka, jika pemilik data akan memberikan uang atau keuntungan lainnya. Jika pemilik data enggan membayar, peretas mengancam akan menghapus atau mengungkapkan data atau informasi penting mereka.

Kasus Ransomware Bank Syariah Indonesia

Pada tahun 2023, pada PT Bank Syariah Indonesia Tbk terjadi kendala sistem selama empat hari. Berlangsung dari Senin, 8 Mei 2023 hingga Kamis, 11 Mei 2023, sistem kembali pulih sepenuhnya dan nasabah dapat melakukan transaksi seperti biasa. Akibat gangguan sistem ini, sejumlah nasabah mengeluh tentang lamanya gangguan sistem dan tidak bisa melakukan penarikan uang atau transaksi lainnya melalui aplikasi Bank Syariah Indonesia.

Pada Senin, 8 Mei 2023, banyak nasabah mengeluh tidak dapat mengakses layanan yang disediakan oleh PT Bank Syariah Indonesia Tbk. Mereka tidak dapat melakukan transaksi melalui teller di kantor cabang, mesin ATM, maupun BSI Mobile. Pada Selasa, 9

Mei 2023, PT Bank Syariah Indonesia Tbk mengatakan bahwa kendala sistem terjadi karena mereka sedang melakukan perawatan system yang mereka sampaikan melalui akun Instagram resmi mereka, mereka juga meminta maaf kepada nasabah atas ketidaknyamanan yang mereka alami. Namun, pada hari yang sama, BSI menyatakan bahwa layanan perbankan syariah telah pulih secara bertahap, sehingga memungkinkan nasabah untuk melakukan transaksi kembali. Tetapi pada Rabu, 10 Mei 2023, layanan PT Bank Syariah Indonesia Tbk masih belum pulih sepenuhnya, dan aplikasi BSI Mobile masih tidak berfungsi saat dibuka. Pada Kamis, 11 Mei 2023, Hery Gunardi, Direktur Utama BSI menyatakan bahwa layanan PT Bank Syariah Indonesia telah diperbaiki sepenuhnya, dan nasabah dapat melakukan transaksi seperti biasa. Selain itu, Hery mengatakan bahwa BSI telah berusaha keras untuk memperbaiki layanan sejak gangguan tersebut terjadi. Selain itu, ia mengatakan bahwa telah ditemukan dugaan bahwa layanan BSI terganggu karena adanya serangan siber.

Pada Sabtu, 13 Mei 2023, akun Twitter Fusion Intelligence Center melaporkan bahwa kelompok peretas spesialis ransomware LockBit 3.0 telah menyerang sistem layanan BSI. Mereka mengklaim telah mencuri 15 juta data pelanggan, informasi karyawan, dan sekitar 1,5 terabyte data dari sistem BSI. Mereka mengancam pihak manajemen BSI untuk segera menghubungi mereka dalam jangka waktu 72 jam dan meminta untuk membayar tebusan atau mereka akan membocorkan data nasabah yang telah dicuri.

Dilaporkan bahwa kelompok hacker LockBit berhasil meretas jutaan data nasabah PT Bank Syariah Indonesia Tbk atau BSI pada Selasa, 16 Mei 2023. Diduga mereka bahkan telah menyebarkan informasi tersebut melalui pasar gelap internet atau *dark web*. Seperti yang dipublikasikan oleh akun *dark tracer* Twitter, @darktracer_int, LockBit mengklaim telah melakukan negosiasi dengan pihak BSI sebelum menyebarkan data tersebut. Disertakan gambar riwayat pembicaraan antara LockBit dan orang yang diduga berasal dari BSI. Pembicaraan dimulai dengan ancaman LockBit untuk menyebarkan data nasabah yang diretas kecuali BSI membayar tebusan. Kemudian pihak BSI menyatakan kesanggupan dengan membayar sebesar 100.000 dolar AS, atau sekitar Rp 1,48 miliar, dengan asumsi kurs Rp 14.850 per dolar AS. Tawaran tersebut ditolak oleh pihak LockBit dan mereka kemudian meminta tebusan sebesar 20 juta dolar.

Melansir dari liputan6.com, pelaku mengatakan tidak ingin memberikan informasi lebih dalam tentang cara mereka dapat mengakses sistem yang dimiliki BSI.

" *Kami menghindari menyebarkan informasi tentang sistem keamanan BSI dan kebobolan karyawan, jadi kami menyimpan beberapa data untuk diri kami sendiri untuk penggunaan berikutnya.* " tulis kelompok ransomware LockBit.

Pemecahan Kasus

Meskipun pihak manajemen mengakui bahwa BSI telah terkena serangan siber, Komaruddin Hidayat, selaku Komisaris Independen BSI, menyatakan bahwa tuduhan LockBit adalah bohong. Ia juga mengatakan bahwa BSI telah bekerja sama dengan tim ahli untuk mengusut tuntas perkara ini dan seluruh system BSI telah pulih serta keamanan data dan uang nasabah aman.

Direktur utama BSI, Hery Gunardi, memberitahukan bahwa pihaknya terus meningkatkan keamanan teknologi perusahaan dengan membentuk divisi khusus yang berada di bawah CISO (Chief Information and Security Officer).

Meskipun begitu dari fenomena diatas, perlindungan terhadap layanan perbankan dari serangan siber menjadi sangat penting. Upaya pencegahan yang proaktif, deteksi dini, respons cepat, penerapan teknologi yang aman, dan penerapan kebijakan keamanan data yang kuat menjadi elemen krusial dalam menjaga integritas dan keamanan transaksi keuangan.

KESIMPULAN

Ransomware tidak hanya menyebabkan kerugian finansial yang besar tetapi juga merusak reputasi lembaga keuangan, mengganggu efisiensi operasional serta masalah semacam ini dapat menimbulkan ketidaknyamanan dan kurangnya kepercayaan terhadap layanan perbankan online. Dan satu lagi, konsekuensi seriusnya adalah dapat menimbulkan kerugian berupa penyalahgunaan data pengguna dan jaringan. Dengan kemajuan ilmu pengetahuan dan teknologi, semakin banyak individu yang berusaha mencapai tujuan mereka dalam jangka waktu singkat, baik dengan cara yang benar maupun salah. Oleh karena itu, sangat penting bagi layanan perbankan untuk memahami serangan ransomware dan bahayanya ransomware.

Beberapa Cara Mengatasi Ransomware:

1. Berhati-hati dalam membuka iklan karena, ransomware dapat menyerang melalui iklan, begitu korban klik iklan tersebut, ransomware langsung ter-instal pada perangkat korban. Sama seperti tautan yang mencurigakan, korban harus berhati-hati juga untuk tidak mengklik tautan dan iklan yang tidak perlu.
2. Alat keamanan jaringan seperti firewall dan antivirus dapat berfungsi sebagai perlindungan keamanan yang wajib untuk perangkat korban sepanjang waktu.
3. Tidak mengakses situs web sembarangan karena, korban dapat menghadapi banyak risiko jika mereka mengakses situs web tidak resmi yang tersebar luas di internet. Seperti

kemungkinan serangan virus. Ransomware juga dapat menyerang file yang ada di situs web tidak resmi dan menunggu korban mengunduh file berbahaya tersebut.

4. Secara teratur membuat salinan cadangan data dan simpan salinan tersebut di lokasi yang aman dan berbeda dengan komputer utama milik korban. Dengan cara ini, korban masih dapat mengembalikan datanya dari salinan cadangan jika terjadi serangan ransomware.
5. Beritahu seluruh pengguna komputer mengenai bahaya ransomware dan ajarkan mereka cara membedakan email phishing atau tautan yang mencurigakan. Semakin tinggi kesadaran pengguna, semakin kecil kemungkinan serangan ransomware terjadi.
6. Berikan hak akses yang tepat kepada pengguna di jaringan korban. Dengan membatasi hak akses administratif ke file dapat mengurangi dampak serangan ransomware ketika akun pengguna terkena dampak serangan.

DAFTAR PUSTAKA

Farid, A. (2022, Oktober 8). *3 Strategi Penerapan Cyber Security Dunia Perbankan*. Retrieved from www.exabyte.co.id:https://www.exabytes.co.id/blog/penerapan-cyber-security-dunia-perbankan/

Harmen, F. A. (2023, juni 12). *Ransomware, Ancaman dan Langkah-Langkah untuk Menghindarinya*. Retrieved from djpk.kemenkeu.go.id: https://www.djkn.kemenkeu.go.id/kanwil-jabar/baca-artikel/16188/Ransomware-Ancaman-dan-Langkah-Langkah-untuk-Menghindarinya.html

Hartono, B. (2023). Ransomware: Memahami Ancaman Keamanan Digital. *Bincang Sains dan Teknologi (BST)*, 55-62.

Johnson, K., & Putih, L. (2021). *Ancaman Keamanan Siber dalam Layanan Perbankan Online: Tinjauan Risiko yang Muncul. Jurnal Keamanan Finansial*, 9(3), 67-78.

Muftiadi, A., Agustina, T. P., & Evi, M. (2022). Studi kasus keamanan jaringan komputer: analisis ancaman phising terhadap layanan online banking. *Jurnal Ilmiah Teknik*, 61-63.

Muhtar. (2023, Mei 23). *Mengenal Ransomware; Cara Kerja dan Tips Pencegahannya*. Retrieved from uic.ac.id: https://uici.ac.id/mengenal-ransomware-cara-kerja-dan-tips-pencegahannya/

Respati, A. R., & Sukmana, Y. (2023, Mei 17). *Perjalanan Kasus BSI, dari Gangguan Layanan sampai "Hacker" Minta Tebusan*. Retrieved from Kompas.com: https://money.kompas.com/read/2023/05/17/072027926/perjalanan-kasus-bsi-dari-gangguan-layanan-sampai-hacker-minta-tebusan?page=all

Syahputra, E. (2021, Desember 1). *Perlu Cara Jenius Mengatasi Kejahatan Siber Perbankan*. www.cnbcindonesia.com:https://www.cnbcindonesia.com/tech/20211201161804-37-295890/perlu-cara-jenius-mengatasi-kejahatan-siber-perbankan

Wardani, A. S. (2024, Januari 14). *Pakar Sebut BSI Jadi Korban Ransomware, 1,5 TB Data Milik 15 Juta Nasabah Dicuri dan Hacker Minta Tebusan*. Retrieved from www.liputan6.com: https://www.liputan6.com/tekno/read/5285443/pakar-sebut-bsi-jadi-korban-ransomware-15-tb-data-milik-15-juta-nasabah-dicuri-dan-hacker-minta-tebusan

Wang, Q., & Liu, M. (2020). *Mitigasi Risiko Siber di Perbankan: Strategi dan Praktik Terbaik. Jurnal Internasional Teknologi Perbankan*, 8(1), 34-47.

www.acerid.com. (2023, Juni 6). *Ransomware :Cara Kerja, Contoh, hingga Mengatasi Serangan*. Retrieved from www.acerid.com: https://www.acerid.com/bisnis/cara-kerja-ransomware-hingga-cara-mengatasinya