ANALISIS KASUS

SERANGAN RANSOMWARE TERHADAP BANK SYARIAH INDONESIA (BSI)

TOBIAS MIKHA SULISTIYO
12024002503

PROGRAM STUDI MAGISTER TEKNIK ELEKTRO
FAKULTAS BIOSAINS
UNIVERSITAS KATOLIK INDONESIA ATMA JAYA
JAKARTA
2025

Analisis Kasus

Serangan *Ransomware* Terhadap Bank Syariah Indonesia (BSI)

1. Latar Belakang

Pada tanggal 8 Mei 2023, Bank Syariah Indonesia (BSI) mengalami serangan siber besar-besaran yang diduga berasal dari kelompok *ransomware LockBit 3.0*. Serangan ini menyebabkan lumpuhnya hampir seluruh layanan digital bank, termasuk ATM, mobile banking, dan internet banking, yang berlangsung selama hampir satu pekan. Gangguan ini berdampak signifikan pada nasabah di seluruh Indonesia, memicu antrean panjang di kantor cabang dan menurunkan kepercayaan publik terhadap sistem perbankan digital [1], [2].

Lebih lanjut, insiden ini mengakibatkan pencurian sekitar 1,5 *terabyte* data yang mencakup informasi pribadi dan rahasia milik sekitar 15 juta nasabah dan pegawai. Data yang dibobol antara lain terdiri dari nama lengkap, alamat, nomor rekening, PIN, kredensial internal, dokumen finansial seperti laporan keuangan, hingga dokumen legal penting yang disimpan dalam sistem internal BSI [3], [4]. Hal ini menunjukkan bahwa peretas memiliki akses mendalam ke berbagai sistem inti dan file sensitif, yang seharusnya dilindungi dengan pengamanan berlapis.

Dalam kasus ini, kelompok penyerang menuntut tebusan sebesar USD 20 juta kepada pihak BSI untuk menghentikan penyebaran data dan memberikan kunci dekripsi. LockBit juga mengancam akan mempublikasikan data curian ke dark web jika permintaan tidak dipenuhi dalam jangka waktu tertentu [5], [6]. Beberapa laporan menyebutkan bahwa sebagian dari data tersebut telah mulai tersebar secara daring, memperbesar risiko penyalahgunaan data oleh pihak ketiga.

Serangan ini menjadi bukti nyata lemahnya kontrol keamanan siber di sektor keuangan yang sangat bergantung pada digitalisasi. Kegagalan dalam mendeteksi dan mengatasi ancaman siber seperti ini menunjukkan bahwa sistem pertahanan siber BSI tidak cukup tangguh untuk menahan metode serangan modern yang semakin canggih. Kasus ini pun memicu diskusi publik mengenai perlindungan data pribadi di Indonesia serta efektivitas regulasi yang sudah ada, seperti Undang-Undang Perlindungan Data Pribadi (UU PDP) [7], [8].

2. Teori

2.1. CIA Triad

Konsep *Confidentiality, Integrity, Availability (CIA Triad)* merupakan kerangka dasar dalam keamanan informasi yang digunakan untuk mengevaluasi dan mengklasifikasikan dampak dari insiden siber. Kerangka ini menjelaskan bagaimana data dan sistem informasi harus dikelola dan dilindungi agar tetap aman dari ancaman, baik yang berasal dari luar

maupun dari dalam organisasi. Dalam konteks serangan *ransomware* terhadap Bank Syariah Indonesia (BSI), ketiga elemen CIA mengalami gangguan signifikan yang berdampak luas terhadap sistem perbankan dan kepercayaan publik.

Confidentiality atau kerahasiaan data menjadi aspek paling terdampak dalam kasus BSI. Sekitar 1,5 terabyte data pribadi milik sekitar 15 juta nasabah dan pegawai telah berhasil dicuri oleh pelaku. Data yang bocor mencakup informasi sensitif seperti nama lengkap, alamat, nomor rekening, PIN, riwayat transaksi, dan dokumen legal lainnya. Menurut teori keamanan informasi, ketika kerahasiaan dilanggar, risiko yang muncul meliputi pencurian identitas, penipuan keuangan, hingga eksploitasi data oleh pihak ketiga [5], [9], [10]. Bahkan, dalam beberapa kasus, kebocoran data dapat menyebabkan kriminalisasi terhadap korban karena data pribadi mereka disalahgunakan oleh pelaku [10].

Integrity atau integritas data juga menjadi perhatian utama. Dalam laporan pasca insiden, diketahui bahwa penyerang berhasil mengakses sistem melalui komputer yang bukan server utama, melainkan perangkat internal pegawai yang tidak seharusnya memiliki akses langsung ke data sensitif [2]. Secara teori, pelanggaran terhadap integritas dapat memungkinkan manipulasi terhadap data keuangan, riwayat transaksi, dan kredensial tanpa dapat dideteksi secara real-time. Tanpa adanya sistem audit yang kuat dan monitoring yang aktif, risiko rekayasa data, pengubahan nilai saldo, atau penyisipan transaksi palsu sangat tinggi [1], [3].

Dampak terhadap *Availability* atau ketersediaan layanan pun tidak kalah besar. Selama hampir satu pekan, layanan penting seperti *mobile banking, internet banking,* dan ATM BSI mengalami kelumpuhan total. Gangguan ini menyebabkan antrean panjang nasabah di kantor cabang dan bandara, serta meningkatkan keresahan publik akibat terhambatnya aktivitas ekonomi yang bergantung pada layanan keuangan digital [4], [10]. Dalam kerangka CIA, ketersediaan sistem sangat krusial agar layanan tetap berjalan dan dapat diakses oleh pengguna saat dibutuhkan. Gangguan jangka panjang pada aspek ini dapat mengakibatkan kerugian finansial, reputasi, serta kehilangan nasabah secara permanen.

Secara keseluruhan, kegagalan dalam menjaga ketiga aspek CIA menunjukkan adanya celah serius dalam tata kelola keamanan informasi di lingkungan perbankan. Serangan *ransomware* seperti ini memanfaatkan lemahnya segmentasi jaringan, kurangnya kontrol akses, serta kelalaian dalam menerapkan prinsip *least privilege*. Dalam perspektif teori manajemen risiko, ketidaksiapan menghadapi ancaman internal dan eksternal memperbesar kemungkinan terjadinya insiden dengan dampak luas, terutama dalam sektor-sektor vital seperti perbankan [2], [3].

Untuk itu, penerapan prinsip-prinsip CIA harus menjadi landasan utama dalam desain arsitektur keamanan informasi. Setiap akses terhadap data harus diatur dengan sistem autentikasi berlapis dan pemantauan berkelanjutan, serta dilakukan audit secara berkala untuk mendeteksi potensi pelanggaran integritas. Ketersediaan sistem pun perlu dijaga melalui infrastruktur cadangan dan *disaster recovery plan* yang matang. Kasus BSI menjadi bukti konkret bahwa pengabaian terhadap kerangka CIA dapat berdampak sangat merugikan bagi organisasi maupun publik secara luas [1], [6], [8].

2.2. Pendekatan UU PDP

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) merupakan tonggak penting dalam perlindungan hak privasi masyarakat Indonesia di era digital. UU ini menetapkan bahwa setiap pengendali data wajib memberitahukan kepada pemilik data apabila terjadi insiden kebocoran, tanpa penundaan yang tidak perlu. Notifikasi tersebut harus disertai informasi mengenai jenis data yang terdampak, waktu terjadinya kebocoran, serta langkah-langkah mitigasi yang dilakukan oleh pengendali data [7], [8]. Dalam konteks serangan siber terhadap BSI, keterlambatan atau ketidakhadiran laporan resmi kepada publik dan otoritas terkait menjadi salah satu isu krusial yang memperkuat dugaan pelanggaran terhadap pasal ini.

Salah satu elemen penting dari UU PDP adalah adanya sanksi administratif dan pidana bagi pelanggar kewajiban perlindungan data. Pasal 57 dan 58 UU PDP memberikan wewenang kepada lembaga pengawas untuk menjatuhkan sanksi berupa teguran tertulis, penghentian sementara aktivitas pemrosesan data, penghapusan data pribadi, dan bahkan denda administratif hingga 2% dari pendapatan tahunan. Selain itu, terdapat ancaman sanksi pidana berupa denda antara Rp4 hingga Rp6 miliar dan hukuman penjara antara 4 hingga 6 tahun bagi pengendali data yang lalai atau sengaja melanggar ketentuan [8]. Oleh karena itu, jika terbukti BSI tidak melakukan kewajibannya sesuai Pasal 46 ayat (2), maka institusi tersebut berpotensi dikenai sanksi sesuai yang diatur dalam regulasi tersebut.

Kasus kebocoran data pada BSI merupakan salah satu ujian praktis pertama terhadap penerapan UU PDP di Indonesia. Sebagai bank syariah nasional hasil merger dengan cakupan layanan besar, BSI memiliki tanggung jawab hukum dan moral untuk memastikan perlindungan maksimal terhadap data pribadi nasabah dan pegawainya. Ketiadaan transparansi informasi pasca-serangan justru membuka peluang terjadinya krisis kepercayaan dari publik. Hal ini memperkuat argumentasi bahwa UU PDP seharusnya tidak hanya menjadi payung hukum, tetapi juga instrumen pengawasan yang tegas oleh lembaga seperti Kominfo, BSSN, dan OJK [1], [7], [8].

Apabila pendekatan hukum yang diambil pemerintah bersifat pasif, maka potensi *class action* atau tuntutan hukum secara kolektif dari nasabah terhadap BSI dapat muncul. Meskipun secara kultur gugatan massal belum umum di Indonesia, tren global dan kesadaran masyarakat akan hak data pribadi semakin meningkat. Dalam banyak negara, pelanggaran atas kerahasiaan data pribadi kerap memicu litigasi besar dengan konsekuensi finansial dan reputasi yang sangat signifikan bagi institusi keuangan [8]. Situasi ini menjadi peringatan bagi sektor industri digital dan finansial bahwa pengabaian terhadap kewajiban perlindungan data bisa berujung pada krisis sistemik yang merugikan semua pihak.

Lebih jauh, dalam teori hukum siber, aspek akuntabilitas menjadi komponen penting dalam penerapan prinsip keadilan digital. Tanpa sistem pelaporan yang transparan dan mekanisme pertanggungjawaban yang tegas, UU PDP tidak akan mampu memberikan perlindungan yang efektif kepada subjek data. Maka dari itu, penerapan prinsip *privacy by design* dan *privacy by default* perlu diterapkan sejak awal dalam sistem pengolahan data

di lembaga keuangan seperti BSI, agar sejalan dengan prinsip-prinsip perlindungan data yang telah diadopsi secara internasional, seperti GDPR di Uni Eropa [7], [8].

Dengan demikian, kasus BSI menjadi studi nyata bahwa UU PDP bukan sekadar produk hukum formal, melainkan instrumen strategis untuk membentuk budaya digital yang lebih bertanggung jawab dan transparan. UU ini juga menuntut adanya kesiapan teknis, kebijakan internal yang adaptif, serta pemahaman yang menyeluruh dari seluruh lapisan organisasi terhadap perlindungan data pribadi. Jika tidak diimplementasikan dengan benar, UU PDP berisiko menjadi aturan yang lemah dan tidak berdampak, justru di saat masyarakat sangat membutuhkannya untuk menjamin hak privasi mereka [1], [7], [8].

3. Solusi

Sebagai tanggapan atas insiden serangan *ransomware* terhadap Bank Syariah Indonesia (BSI), perlu diterapkan pendekatan komprehensif yang mencakup aspek respons, pemulihan, pencegahan, dan penguatan kebijakan kelembagaan. Langkah pertama yang harus dilakukan adalah membentuk tim tanggap insiden (Incident Response Team) yang bekerja sesuai dengan prosedur *Incident Response Plan (IRP)*. Sistem yang terdampak perlu segera diisolasi untuk mencegah penyebaran malware lebih lanjut, disertai dengan proses audit log, investigasi forensik digital, serta pelibatan lembaga pengawas seperti BSSN dan OJK guna memastikan transparansi dan akuntabilitas penanganan [1], [2]. Selain itu, sesuai ketentuan dalam UU PDP, lembaga pengendali data wajib memberikan notifikasi resmi kepada nasabah dan regulator mengenai jenis data yang bocor serta langkah mitigasi yang telah diambil [7], [8].

Dari sisi teknis, solusi utama yang dapat mencegah serangan serupa di masa depan adalah penerapan model keamanan *zero-trust architecture* yang mengharuskan validasi akses secara ketat, menghilangkan akses langsung ke database dari perangkat non-server, serta implementasi otentikasi multifaktor (MFA) dan segmentasi jaringan [1], [2]. Untuk menjaga aspek *availability*, institusi seperti BSI juga harus memvalidasi sistem cadangan dan pemulihan bencana (*backup and disaster recovery plan*) secara berkala, termasuk melalui uji coba pemulihan dari backup offline untuk memastikan data tetap utuh dan dapat digunakan ketika sistem utama terganggu. Ketahanan sistem terhadap serangan siber bergantung tidak hanya pada alat yang digunakan, tetapi juga pada kesiapan menghadapi serangan yang semakin kompleks dan canggih [3].

Langkah preventif jangka panjang memerlukan pembangunan budaya keamanan informasi secara menyeluruh. Pelatihan keamanan siber wajib diberikan kepada seluruh pegawai dan pemangku kepentingan melalui simulasi phishing, pelatihan berkala, dan sertifikasi keamanan digital untuk meningkatkan *security awareness*. Bagi nasabah, edukasi tentang praktik keamanan digital juga perlu ditingkatkan agar mereka mampu mengenali risiko dan tidak menjadi pintu masuk bagi serangan sosial engineering [4], [9]. Selain itu, penguatan sistem proteksi endpoint melalui penerapan EDR/XDR, filter email canggih, serta pemantauan cloud dan trafik jaringan berbasis benchmark seperti CIS dapat memperkuat perimeter pertahanan institusi keuangan [4], [5].

Dari sisi tata kelola, langkah-langkah strategis mencakup evaluasi ulang regulasi keamanan teknologi informasi oleh OJK dan BSSN untuk mendorong peningkatan standar operasional perbankan. Audit keamanan siber terhadap vendor dan pihak ketiga juga perlu dilakukan secara rutin guna menghindari risiko rantai pasok (*supply chain attack*) yang kerap menjadi titik lemah dalam infrastruktur digital [2], [4]. Selain itu, audit dan sertifikasi berstandar internasional seperti ISO 27001 perlu diwajibkan sebagai bagian dari kepatuhan operasional. Sosialisasi UU PDP kepada seluruh industri keuangan dan masyarakat juga menjadi krusial untuk memperkuat literasi perlindungan data pribadi serta menumbuhkan kepercayaan terhadap layanan digital [7], [8]. Dengan demikian, solusi ini tidak hanya bersifat reaktif, tetapi membangun ekosistem keamanan yang berkelanjutan.

4. Kesimpulan

Berdasarkan hasil kajian terhadap serangan *ransomware* yang menimpa Bank Syariah Indonesia (BSI) pada Mei 2023, dapat disimpulkan bahwa insiden ini merupakan cerminan nyata dari lemahnya sistem pertahanan siber di sektor perbankan nasional. Serangan yang diduga berasal dari kelompok LockBit 3.0 tidak hanya melumpuhkan layanan digital selama hampir satu pekan, tetapi juga mengakibatkan kebocoran sekitar 1,5 terabyte data sensitif yang mencakup informasi pribadi nasabah dan pegawai. Dampak dari insiden ini mencakup seluruh aspek dalam kerangka CIA (Confidentiality, Integrity, dan Availability), yang menunjukkan bahwa sistem keamanan digital BSI belum memiliki ketahanan yang memadai terhadap ancaman siber modern.

Analisis terhadap insiden ini juga menunjukkan bahwa implementasi Undang-Undang Perlindungan Data Pribadi (UU PDP) masih belum optimal. Ketidakhadiran notifikasi publik secara cepat dan keterbukaan informasi menandakan bahwa aspek akuntabilitas dan transparansi belum sepenuhnya dijalankan oleh institusi keuangan, padahal regulasi tersebut sudah menetapkan kewajiban perlindungan dan pelaporan bagi setiap pengendali data pribadi. Hal ini memperkuat urgensi untuk menegakkan UU PDP sebagai pilar utama dalam perlindungan hak privasi digital masyarakat Indonesia.

Solusi yang disusun dari perspektif cybersecurity officer menunjukkan bahwa pendekatan ideal terhadap insiden seperti ini mencakup tiga aspek: tanggap insiden dan pemulihan, strategi pencegahan teknis, serta perbaikan tata kelola dan kepatuhan hukum. Penerapan arsitektur keamanan zero-trust, validasi berkala terhadap sistem cadangan, pelatihan keamanan siber, dan penguatan regulasi menjadi bagian integral dalam membangun ketahanan siber yang holistik dan berkelanjutan di sektor keuangan.

5. Saran

Sebagai langkah konkret, institusi keuangan di Indonesia, termasuk BSI, perlu menjadikan keamanan siber sebagai prioritas strategis, bukan sekadar pelengkap teknologi. Pembentukan tim tanggap insiden permanen, integrasi sistem forensik digital, serta pelaporan insiden secara proaktif kepada publik dan regulator harus menjadi standar

operasional yang tidak bisa ditawar. Selain itu, seluruh pegawai dan nasabah perlu dibekali literasi keamanan digital untuk mengurangi risiko serangan berbasis rekayasa sosial.

Pemerintah, melalui OJK dan BSSN, juga disarankan untuk melakukan evaluasi menyeluruh terhadap standar keamanan informasi perbankan nasional. Penguatan audit dan kewajiban sertifikasi seperti ISO 27001 perlu diberlakukan secara ketat. Lebih penting lagi, sosialisasi UU PDP harus ditingkatkan kepada seluruh pelaku industri dan masyarakat agar kepatuhan terhadap perlindungan data pribadi dapat menjadi budaya, bukan sekadar kewajiban hukum.

Setiap institusi juga harus memiliki sistem cadangan dan pemulihan bencana (*backup and disaster recovery plan*). Tentunya setelah memiliki system *backup and disaster recovery plan* perlu dilakukan backup secara berkala, termasuk melalui uji coba pemulihan dari *backup offline* untuk memastikan data tetap utuh dan dapat digunakan ketika sistem utama terganggu. Institusi juga harus memiliki sistem ataupun aplikasi cadangan sebagai pencegahan apabila aplikasi utama bermasalah. Prosedur dan uji coba untuk sinkronisasi aplikasi utama dan aplikasi cadangan perlu diberlakukan secara berkala.

Dengan sinergi antara teknologi, sumber daya manusia, regulasi, dan kesadaran publik, diharapkan Indonesia mampu menghadapi tantangan keamanan digital yang semakin kompleks, serta mencegah insiden serupa terulang kembali di masa mendatang.

6. Referensi

[1] Tekno Tempo, “Pasca Serangan Ransomware BSI, Rombak Direksi IT dan Celah Fatal dari Komputer Karyawan,” *Tempo.co*, 2023. [Online]. Available: https://www.tempo.co/digital/pasca-serangan-ransomware-bsi-rombak-direksi-it-dan-celah-fatal-dari-komputer-karyawan-185190

[2] Bisnis.com, "Kronologi BSI Diserang Ransomware oleh Hacker Lockbit 3.0, Diduga Beraksi Sejak Libur Lebaran 2023," *Bisnis.com*, 2023. [Online]. Available: https://finansial.bisnis.com/read/20230514/90/1655733/kronologi-bsi-diserang-ransomware-oleh-hacker-lockbit-30-diduga-beraksi-sejak-libur-lebaran-2023

[3] Direktorat Jenderal Kekayaan Negara, “BSI dan Serangan Siber: Perlunya Tata Kelola Keamanan Data,” *djkn.kemenkeu.go.id*, 2023. [Online]. Available: https://www.djkn.kemenkeu.go.id/

[4] Januar Rizki, “Lima Langkah Penanganan Data Pribadi Sesuai Regulasi atas Dugaan Kebocoran Data BSI,” *Hukumonline.com*, 2023. [Online]. Available: https://www.hukumonline.com/berita/a/lima-langkah-penanganan-data-pribadi-sesuai-regulasi-atas-dugaan-kebocoran-data-bsi-lt6463960943a71/

[5] Tirto.id, “Kronologi LockBit Diduga Curi Data Nasabah BSI & Update Terkini,” *Tirto.id*, 2023. [Online]. Available: https://tirto.id/kronologi-lockbit-diduga-curi-data-nasabah-bsi-update-terkini-gHpm

[6] Tempo Tekno, “Beredar Chat LockBit Minta Tebusan Rp 295 Miliar ke BSI,” *Tempo.co*, 2023. [Online]. Available: https://www.tempo.co/digital/beredar-chat-lockbit-minta-tebusan-rp-295-miliar-ke-bsi-187033

[7] Gizmologi, “Ujian UU PDP, ELSAM Desak BSSN Gercep Tangani Ransomware BSI,” *Gizmologi.id*, 2023. [Online]. Available: https://gizmologi.id/news/elsam-desak-bssn-tangani-ransomware-bsi/

[8] Context ID, “BSI Kena Serangan Siber, Efektifkah UU PDP?,” *Context.id*, 2023. [Online]. Available: https://context.id/read/999/bsi-kena-serangan-siber-efektifkah-uu-pdp

[9] Suryo Anggoro, “Data Nasabah BSI Diduga Bocor karena Ransomware, Harus Bagaimana?,” *detik.com*, 2023. [Online]. Available: https://inet.detik.com/security/d-6718351/data-nasabah-bsi-diduga-bocor-karena-ransomware-harus-bagaimana/

[10] Tempo, “15 Juta Data Nasabah BSI Diduga Bocor, Pakar Siber: Hati-hati Serangan Phising ke Pemilik Rekening,” *tempo.co*, 2023. [Online]. Available: https://www.tempo.co/ekonomi/15-juta-data-nasabah-bsi-diduga-bocor-pakar-siber-hati-hati-serangan-phising-ke-pemilik-rekening-187193