MANTAP: Journal of Management Accounting, Tax and Production
E-ISSN: 3025-7786 P-ISSN: 3025-7794
Vol. 4 No. 1 Maret 2026

Analisis Keamanan Siber Perbankan dan Peran OJK: Studi Kasus Serangan Ransomware pada Bank Syariah Indonesia Tahun 2023

Cantika Sarma Seicilia Silalahi[1] Agni Maria Veronika Manullang[2] Nazira Maulidia Nasution[3] Lia Oktafriani Pandiangan[4] Geby Natalia Butar Butar[5]
Programm Studi Ilmu Ekonomi, Fakultas Ekonomi, Universitas Negeri Medan, Indonesia[1,2,3,4,5]
Email: cantikasilalahi416@gmail.com[1] agnimaria.7242240003@mhs.unimed.ac.id[2]
maulidianazira434@gmail.com[3] liaoktafriani3@gmail.com[4]
gebynatalia.7243240033@mhs.unimed.ac.id[5]

Abstrak
Perkembangan teknologi digital membawa dampak ganda bagi sektor perbankan di satu sisi mempermudah layanan keuangan, namun di sisi lain membuka celah terhadap ancaman siber yang kian serius. Hal ini terbukti dari serangan ransomware yang menimpa Bank Syariah Indonesia (BSI) pada tahun 2023, yang tidak hanya melumpuhkan layanan perbankan tetapi juga menggoyahkan kepercayaan nasabah terhadap keamanan sistem digital. Penelitian ini bertujuan mengkaji kasus tersebut secara mendalam sekaligus melihat sejauh mana peran OJK dalam menjaga ketahanan sistem perbankan nasional, menggunakan pendekatan kualitatif berbasis studi pustaka dan analisis sumber data sekunder. Temuan penelitian menunjukkan bahwa serangan ransomware mampu memberikan dampak yang sangat signifikan, mulai dari terganggunya operasional bank hingga ancaman terhadap stabilitas sistem keuangan secara luas. OJK sebagai regulator memegang peran krusial dalam mendorong perbankan untuk terus memperbarui dan memperkuat infrastruktur keamanan teknologi informasi mereka. Oleh sebab itu, evaluasi sistem secara rutin dan pengelolaan risiko yang lebih matang menjadi langkah yang tidak bisa lagi ditunda oleh industri perbankan Indonesia.
Kata Kunci: Keamanan Siber, Ransomware, Perbankan, Bank Syariah Indonesia, OJK

PENDAHULUAN

Perkembangan teknologi informasi telah mendorong perubahan yang cukup mendasar di berbagai bidang kehidupan, tak terkecuali di sektor perbankan. Saat ini, layanan perbankan tidak lagi terbatas pada kegiatan tatap muka di kantor cabang, melainkan sudah bergeser ke platform digital seperti mobile banking, internet banking, dan beragam fasilitas transaksi elektronik lainnya. Pergeseran ini tentu memberikan kemudahan yang nyata bagi masyarakat, karena transaksi keuangan kini bisa dilakukan dengan lebih cepat, praktis, dan efisien tanpa harus terikat waktu maupun tempat. Meski demikian, di balik segala kemudahan yang ditawarkan, adopsi teknologi digital dalam dunia perbankan juga memunculkan tantangan tersendiri yang tidak bisa dianggap sepele, terutama yang menyangkut keamanan sistem informasi dan perlindungan data para nasabah. Seiring terus meluasnya penggunaan teknologi digital di sektor keuangan, ancaman terhadap keamanan siber pun turut mengalami peningkatan yang cukup signifikan. Berbagai bentuk serangan siber kini semakin sering terjadi, mulai dari upaya peretasan sistem, pencurian data sensitif, hingga serangan ransomware yang berpotensi menghentikan seluruh operasional sebuah lembaga keuangan secara tiba-tiba. Kondisi ini patut menjadi perhatian serius, mengingat sektor perbankan adalah salah satu bidang yang paling bergantung pada keandalan infrastruktur teknologi informasi. Jika pengelolaan keamanan sistem tidak dilakukan secara optimal, maka dampaknya tidak hanya berupa kerugian finansial semata, tetapi juga dapat mengikis kepercayaan masyarakat terhadap lembaga perbankan itu sendiri.

Salah satu peristiwa yang sempat menyita perhatian luas adalah serangan ransomware yang dialami oleh Bank Syariah Indonesia (BSI) pada tahun 2023. Akibat serangan tersebut, sejumlah layanan perbankan mengalami gangguan serius sehingga para nasabah tidak dapat mengakses fasilitas transaksi secara normal dalam kurun waktu tertentu. Kejadian ini secara nyata membuktikan bahwa ancaman keamanan siber bukanlah isu yang bisa diremehkan, karena dampaknya bisa langsung dirasakan oleh operasional bank sehari-hari sekaligus mempengaruhi tingkat kepercayaan masyarakat terhadap sistem perbankan berbasis digital. Menghadapi berbagai risiko siber yang terus berkembang, kehadiran lembaga pengawas yang kuat menjadi suatu kebutuhan yang tidak bisa ditawar. Otoritas Jasa Keuangan (OJK) sebagai regulator sektor keuangan di Indonesia memiliki tanggung jawab besar dalam memastikan bahwa setiap lembaga perbankan telah menerapkan sistem keamanan teknologi informasi yang memadai dan sesuai standar. Atas dasar itulah, penelitian ini berupaya untuk menganalisis secara lebih mendalam kasus serangan ransomware yang menimpa Bank Syariah Indonesia, sekaligus mengkaji bagaimana peran OJK dalam menjaga dan mengawasi keamanan sistem perbankan di Indonesia.

Rumusan Masalah

Merujuk pada latar belakang yang telah dipaparkan sebelumnya, penelitian ini memusatkan perhatian pada beberapa pokok permasalahan yang berkaitan erat dengan isu keamanan siber di lingkungan perbankan. Permasalahan pertama yang ingin ditelusuri adalah bagaimana kronologi serangan ransomware yang menimpa Bank Syariah Indonesia pada tahun 2023 berlangsung, serta seberapa besar dampak yang ditimbulkannya terhadap operasional bank maupun kepercayaan masyarakat. Permasalahan kedua menyangkut faktor-faktor apa saja yang menjadi penyebab atau pemicu terjadinya serangan siber terhadap sistem perbankan, sehingga dapat dipahami dari sisi mana celah kerentanan itu muncul. Di samping itu, penelitian ini turut mengkaji bagaimana Otoritas Jasa Keuangan menjalankan fungsi pengawasannya serta langkah-langkah konkret apa yang telah dan perlu dilakukan guna memperkuat keamanan sistem perbankan di Indonesia secara menyeluruh.

Tujuan Penelitian

Penelitian ini dilakukan dengan tujuan untuk memberikan gambaran yang jelas mengenai kondisi kredit bermasalah yang terjadi pada Bank BRI dalam rentang waktu yang menjadi fokus pengamatan. Secara lebih spesifik, penelitian ini ingin menelusuri bagaimana perkembangan rasio Non Performing Loan pada Bank BRI selama kurun waktu tahun 2020 sampai dengan tahun 2023. Tidak hanya itu, penelitian ini juga berupaya untuk menganalisis faktor-faktor apa saja yang melatarbelakangi terjadinya kredit macet, mengidentifikasi pencapaian yang berhasil diraih oleh pihak bank dalam mengelola portofolio kreditnya, serta memahami berbagai hambatan dan tantangan yang kerap dihadapi dalam proses penyaluran kredit kepada nasabah. Melalui serangkaian tujuan tersebut, penelitian ini diharapkan mampu menghasilkan pemahaman yang lebih komprehensif dan mendalam mengenai strategi-strategi yang diterapkan oleh bank dalam menghadapi dan mengatasi persoalan kredit bermasalah.

Manfaat Penelitian

Penelitian ini diharapkan mampu memberikan kontribusi yang berarti, baik dari sisi akademis maupun praktis. Dari sudut pandang akademis, penelitian ini diharapkan dapat memperluas wawasan dan memperkaya pemahaman mengenai isu keamanan siber di sektor perbankan, khususnya yang berkaitan dengan ancaman serangan ransomware yang semakin marak terjadi. Selain itu, penelitian ini juga diharapkan dapat dijadikan sebagai salah satu rujukan atau referensi bagi mahasiswa maupun peneliti lain yang memiliki ketertarikan untuk

mengkaji lebih jauh topik seputar keamanan teknologi informasi dalam lingkungan industri keuangan. Sementara itu, dari sisi praktis, penelitian ini diharapkan dapat memberikan gambaran yang lebih nyata mengenai betapa pentingnya upaya penguatan sistem keamanan siber di lingkungan lembaga perbankan. Di samping itu, penelitian ini juga diharapkan mampu memberikan informasi yang berguna mengenai bagaimana Otoritas Jasa Keuangan menjalankan fungsi pengawasannya serta mendorong peningkatan standar keamanan teknologi informasi di sektor perbankan, sehingga risiko terjadinya serangan siber di masa mendatang dapat ditekan seminimal mungkin.

Tinjauan Pustaka

Keamanan Siber dalam Sektor Perbankan

Keamanan siber pada dasarnya merupakan serangkaian upaya yang dirancang untuk melindungi sistem komputer, jaringan komunikasi, serta berbagai data penting dari ancaman-ancaman digital yang terus berkembang, seperti peretasan sistem, pencurian informasi sensitif, maupun penyalahgunaan infrastruktur teknologi informasi. Dalam konteks sektor perbankan, keamanan siber menempati posisi yang sangat krusial mengingat hampir seluruh aktivitas operasional perbankan saat ini sudah sangat bergantung pada pemanfaatan teknologi informasi. Keterhubungan sistem perbankan dengan jaringan internet secara tidak langsung menjadikan lembaga keuangan sebagai salah satu sasaran yang paling sering diincar oleh para pelaku kejahatan siber. Atas dasar itulah, setiap bank dituntut untuk memiliki sistem keamanan yang kokoh dan handal guna melindungi data nasabah sekaligus memastikan stabilitas layanan keuangan tetap terjaga dengan baik.

Ransomware

Ransomware merupakan salah satu bentuk serangan siber yang cara kerjanya cukup meresahkan pelaku akan mengunci atau mengenkripsi sistem komputer milik korban sehingga seluruh akses terhadap data maupun sistem tersebut menjadi terblokir sepenuhnya. Setelah berhasil menguasai sistem, pelaku biasanya akan menuntut sejumlah uang tebusan sebagai syarat agar sistem korban dapat dipulihkan dan bisa kembali digunakan seperti semula. Dampak yang ditimbulkan oleh serangan ransomware ini bisa sangat serius, terlebih bagi institusi yang operasionalnya sangat bertumpu pada keandalan sistem teknologi informasi, seperti halnya lembaga perbankan. Apabila sistem sebuah bank berhasil disusupi oleh serangan ransomware, maka berbagai layanan vital seperti transaksi keuangan, mobile banking, hingga akses terhadap data nasabah berpotensi terhenti dalam waktu yang tidak dapat dipastikan. Kondisi semacam ini tentu tidak hanya berdampak pada kerugian finansial yang bisa dialami oleh bank maupun nasabahnya, tetapi juga secara perlahan dapat menggerus kepercayaan masyarakat terhadap keamanan dan keandalan lembaga perbankan yang bersangkutan.

Peran Otoritas Jasa Keuangan dalam Pengawasan Perbankan

Otoritas Jasa Keuangan atau yang lebih dikenal dengan sebutan OJK merupakan lembaga resmi yang diberi mandat untuk mengatur sekaligus mengawasi seluruh kegiatan di sektor jasa keuangan Indonesia, termasuk di dalamnya industri perbankan. Dalam kaitannya dengan isu keamanan siber, OJK memegang peranan penting dalam memastikan bahwa setiap lembaga perbankan telah menerapkan sistem manajemen risiko teknologi informasi yang benar-benar memadai dan sesuai standar yang berlaku. Tidak hanya sebatas pengawasan, OJK juga aktif mendorong perbankan untuk terus berbenah dalam memperkuat keamanan sistem digitalnya, melakukan evaluasi secara berkala terhadap infrastruktur teknologi informasi yang dimiliki, serta menerapkan standar-standar keamanan yang relevan dan mampu mengikuti laju perkembangan teknologi yang begitu cepat. Melalui rangkaian upaya pengawasan tersebut,

diharapkan industri perbankan nasional dapat semakin tangguh dan lebih siap dalam mengantisipasi berbagai ancaman keamanan siber yang terus berevolusi dari waktu ke waktu.

METODE PENELITIAN

Penelitian ini menerapkan pendekatan kualitatif yang berlandaskan metode deskriptif sebagai kerangka utama dalam menganalisis kasus serangan ransomware yang menimpa Bank Syariah Indonesia pada tahun 2023. Adapun data yang digunakan seluruhnya merupakan data sekunder yang dihimpun dari berbagai sumber, di antaranya laporan-laporan resmi, artikel ilmiah, pemberitaan media, serta berbagai publikasi yang memiliki relevansi dengan tema keamanan siber di sektor perbankan. Proses pengumpulan data dilakukan melalui studi pustaka, yaitu dengan menelaah secara mendalam berbagai literatur yang berkaitan langsung dengan topik yang diteliti, mencakup jurnal ilmiah, buku referensi, maupun laporan yang diterbitkan oleh lembaga-lembaga terkait. Selanjutnya, data yang telah berhasil dikumpulkan tersebut dianalisis secara deskriptif guna memperoleh pemahaman yang utuh mengenai bagaimana kronologi serangan ransomware itu berlangsung, dampak apa saja yang dirasakan terhadap operasional perbankan, serta bagaimana peran Otoritas Jasa Keuangan dalam menjalankan fungsi pengawasan dan mendorong peningkatan keamanan sistem perbankan secara keseluruhan.

HASIL PENELITIAN DAN PEMBAHASAN

Kronologi Serangan Siber Bank Syariah Indonesia Tahun 2023

Tanggal	Peristiwa
8 Mei 2023	Layanan BSI mulai mengalami gangguan masif sejak pagi hari. Mobile banking BSI, jaringan ATM (lebih dari 1.200 unit), dan layanan kantor cabang tidak dapat diakses oleh nasabah. BSI awalnya menginformasikan gangguan sebagai 'proses pemeliharaan dan peningkatan kualitas layanan' (maintenance).
9–10 Mei 2023	Gangguan berlanjut. Nasabah tidak dapat melakukan transfer, penarikan tunai, pembayaran, maupun akses rekening. Antrian panjang terjadi di kantor-kantor cabang BSI. Direktur Utama BSI Hery Gunardi menyampaikan permohonan maaf dan menyatakan proses normalisasi sedang berlangsung. Para pakar keamanan siber mulai mencurigai adanya serangan ransomware.
11 Mei 2023	Sistem BSI mulai dipulihkan secara bertahap. Namun kepastian mengenai penyebab gangguan belum diungkap secara resmi oleh manajemen BSI kepada publik.
13 Mei 2023	Pendiri Ethical Hacker Indonesia, Teguh Aprianto, mengungkap melalui media sosial bahwa BSI adalah korban ransomware LockBit 3.0, disertai tangkapan layar dari situs dark web LockBit yang mengakui serangan tersebut. Fakta ini memicu gelombang kekhawatiran publik yang besar.
14–16 Mei 2023	LockBit memberikan ultimatum 72 jam kepada BSI untuk bernegosiasi dan membayar tebusan. Memasuki tenggat, negosiasi tidak tercapai. LockBit mulai mempublikasikan sebagian data BSI sebagai bukti serangan di situs dark web mereka.
18 Mei 2023	LockBit secara resmi mengklaim telah mencuri 1,5 terabyte data dari BSI. Data yang bocor mencakup informasi pribadi lebih dari 15 juta nasabah, data 24.437 karyawan, dokumen internal bank, dan kredensial sistem. Tuntutan tebusan ditetapkan sebesar USD 20 juta (± Rp 296 miliar).
22 Mei 2023	OJK, melalui Kepala Eksekutif Friderica Widyasari Dewi, mengumumkan bahwa OJK telah mengirimkan surat resmi kepada BSI untuk meminta keterangan terkait perlindungan konsumen dan keamanan data nasabah. Kemenkominfo juga melakukan klarifikasi.
Pasca Mei 2023	BSI melibatkan PT Bank Mandiri Tbk (pemegang saham pengendali) dan konsultan keamanan siber independen untuk forensik digital. BSI mengalokasikan anggaran besar untuk memperkuat infrastruktur keamanan siber dan memperbarui sistem yang terdampak.

Mengacu pada data kronologi yang tersaji dalam tabel di atas, gangguan pada layanan Bank Syariah Indonesia tercatat mulai terjadi pada tanggal 8 Mei 2023. Pada hari tersebut, sejumlah fasilitas perbankan seperti BSI Mobile, jaringan ATM, serta layanan transaksi di kantor-kantor cabang mendadak tidak bisa diakses oleh para nasabah. Dalam pernyataan awalnya, pihak bank menjelaskan bahwa gangguan yang terjadi disebabkan oleh adanya proses pemeliharaan sistem yang sedang berlangsung. Namun kenyataannya, hingga tanggal 9 dan 10 Mei 2023 gangguan tersebut masih terus berlanjut tanpa tanda-tanda pemulihan, sehingga nasabah tetap tidak bisa melakukan berbagai kegiatan transaksi seperti transfer dana, pembayaran tagihan, maupun sekadar mengakses informasi rekening mereka. Situasi yang berlarut-larut ini tentu saja memicu gelombang keluhan dari berbagai kalangan masyarakat, khususnya nasabah yang dalam kesehariannya sangat mengandalkan layanan perbankan digital untuk memenuhi kebutuhan finansial mereka. Tidak sedikit nasabah yang akhirnya terpaksa mendatangi kantor cabang secara langsung demi bisa melakukan transaksi, yang pada akhirnya menyebabkan antrean panjang di berbagai titik layanan bank.

Memasuki tanggal 11 Mei 2023, sistem perbankan BSI mulai menunjukkan tanda-tanda pemulihan meskipun prosesnya berjalan secara bertahap. Kendati demikian, penyebab sebenarnya dari gangguan tersebut belum juga diungkapkan secara gamblang kepada publik. Informasi terkait dugaan adanya serangan siber baru mulai mencuat pada tanggal 13 Mei 2023, setelah sejumlah peneliti di bidang keamanan siber mengungkap bahwa BSI diduga kuat telah menjadi korban serangan ransomware LockBit 3.0. Perkembangan kasus ini kemudian bergerak semakin serius ketika kelompok peretas yang bertanggung jawab mulai memberikan ultimatum kepada pihak bank untuk segera melakukan negosiasi perihal pembayaran uang tebusan. Puncaknya, pada tanggal 18 Mei 2023 kelompok tersebut secara terbuka mengklaim bahwa mereka telah berhasil mencuri lebih dari 1,5 terabyte data dari sistem internal bank. Berdasarkan rangkaian peristiwa tersebut, terlihat jelas bahwa serangan siber ini tidak semata-mata berdampak pada kekacauan operasional bank, tetapi juga memunculkan kekhawatiran yang mendalam di kalangan nasabah terkait keamanan data pribadi mereka.

Dampak Serangan Siber terhadap Operasional Perbankan

Dimensi Dampak	Indikator	Keterangan
Operasional	Gangguan layanan 2–4 hari	Mobile banking, ATM (>1.200 unit), dan layanan cabang tidak dapat diakses
Operasional	Core banking tidak berfungsi	Seluruh transaksi terhenti; layanan haji terdampak saat musim haji
Data & Privasi	1,5 TB data tercuri	Lebih dari 15 juta data nasabah dan 24.437 data karyawan terekspos
Data & Privasi	Jenis data terdampak	Nama, alamat, nomor telepon, nomor rekening, riwayat transaksi, dokumen KTP
Keuangan	Biaya pemulihan	Biaya forensik digital, pembaruan sistem, dan kompensasi nasabah (belum diungkap resmi)
Keuangan	Potensi denda regulasi	Berdasarkan UU PDP, potensi sanksi administratif atas kegagalan perlindungan data
Reputasi	Kepercayaan nasabah	Survei pasca-insiden menunjukkan penurunan signifikan kepercayaan nasabah BSI
Reputasi	Respons komunikasi dikritisi	Publik mengkritik pernyataan awal BSI yang menyebut gangguan sebagai maintenance

Serangan siber yang menimpa Bank Syariah Indonesia ternyata membawa dampak yang cukup signifikan terhadap keberlangsungan operasional perbankan. Berdasarkan berbagai data yang tersedia, gangguan pada sistem yang terjadi mengakibatkan beragam layanan perbankan tidak dapat dimanfaatkan oleh nasabah selama beberapa hari berturut-turut.

Layanan digital unggulan seperti BSI Mobile sama sekali tidak bisa diakses, sementara jaringan ATM yang jumlahnya mencapai lebih dari 1.200 unit di berbagai wilayah juga turut mengalami gangguan, sehingga nasabah tidak memiliki pilihan lain selain mengurungkan niat untuk melakukan penarikan tunai maupun transaksi-transaksi lainnya. Tidak hanya layanan digital, fasilitas transaksi di kantor-kantor cabang pun ikut terdampak karena sistem perbankan yang menjadi tulang punggung operasional tidak berfungsi sebagaimana mestinya. Keadaan ini memaksa banyak nasabah untuk turun langsung mendatangi kantor cabang terdekat, baik sekadar untuk memperoleh informasi terkini maupun untuk menyelesaikan transaksi secara manual. Alhasil, antrean panjang tidak terhindarkan dan terjadi di berbagai kantor layanan BSI. Gangguan yang berlangsung dalam beberapa hari tersebut jelas memberikan pengaruh nyata terhadap aktivitas transaksi keuangan masyarakat, terutama bagi mereka yang dalam keseharian sudah sangat bergantung pada layanan perbankan digital untuk keperluan pembayaran, transfer dana, maupun berbagai kegiatan ekonomi lainnya. Insiden ini sekaligus menjadi bukti nyata bahwa sistem perbankan yang berbasis teknologi menyimpan risiko yang tidak kecil, terlebih apabila terjadi celah atau kegagalan pada sistem keamanan digitalnya.

Kebocoran Data Nasabah dan Risiko Keamanan Informasi

Di samping mengakibatkan kekacauan pada sisi operasional, serangan ransomware yang menimpa Bank Syariah Indonesia juga memunculkan keresahan yang tidak kalah serius, yakni menyangkut keamanan data milik para nasabah. Berdasarkan informasi yang beredar luas, kelompok peretas LockBit mengklaim telah berhasil mengambil sekitar 1,5 terabyte data dari sistem internal bank. Data yang diduga berhasil dicuri tersebut mencakup berbagai informasi yang sangat sensitif, termasuk data pribadi lebih dari 15 juta nasabah serta kurang lebih 24.437 data karyawan BSI yang tersimpan dalam sistem. Jenis-jenis data yang dilaporkan ikut bocor dalam insiden tersebut terbilang cukup lengkap dan rawan disalahgunakan, mulai dari nama lengkap, alamat tempat tinggal, nomor telepon, nomor rekening, riwayat transaksi, hingga dokumen identitas resmi seperti KTP maupun paspor. Apabila data-data tersebut benar-benar jatuh ke tangan pihak yang tidak bertanggung jawab, maka potensi kerugian yang bisa dialami oleh nasabah sangatlah besar, mulai dari penyalahgunaan identitas hingga berbagai modus penipuan yang dapat merugikan secara finansial maupun non-finansial. Kasus ini pada akhirnya menegaskan bahwa perlindungan data pribadi merupakan salah satu elemen yang tidak bisa diabaikan dalam ekosistem perbankan digital. Bank tidak cukup hanya bertanggung jawab menjaga keamanan dana nasabah semata, tetapi juga memiliki kewajiban untuk memastikan bahwa seluruh data pribadi yang tersimpan dan dikelola dalam sistem teknologi informasinya benar-benar terlindungi secara optimal dari berbagai bentuk ancaman kejahatan siber yang terus berkembang.

Peran Otoritas Jasa Keuangan dalam Penanganan Insiden

Dalam merespons insiden keamanan siber yang dialami oleh Bank Syariah Indonesia, Otoritas Jasa Keuangan selaku lembaga regulator di sektor jasa keuangan memainkan peranan yang sangat vital. OJK memiliki tanggung jawab untuk memastikan bahwa setiap lembaga perbankan mampu menjaga stabilitas sistem keuangan yang ada sekaligus melindungi kepentingan nasabah dari berbagai risiko yang mungkin timbul. Setelah gangguan sistem pada BSI mulai mencuat ke permukaan, OJK tidak tinggal diam dan segera mengambil langkah pengawasan dengan meminta klarifikasi langsung kepada pihak bank terkait akar penyebab gangguan tersebut, sekaligus menanyakan langkah-langkah konkret yang sedang dan akan dilakukan untuk memulihkan layanan perbankan yang terdampak. Lebih dari itu, OJK juga turut memantau secara aktif proses pemulihan sistem yang dijalankan oleh pihak bank demi memastikan seluruh layanan perbankan dapat kembali beroperasi secara normal dalam waktu

yang tidak terlalu lama. Jika dilihat dalam cakupan yang lebih luas, OJK sebenarnya telah terlebih dahulu memiliki sejumlah regulasi yang secara khusus mengatur penerapan teknologi informasi di sektor perbankan, di antaranya Peraturan OJK Nomor 11 Tahun 2022 tentang penyelenggaraan teknologi informasi oleh bank umum, serta Surat Edaran OJK Nomor 29 Tahun 2022 yang mengatur mengenai manajemen risiko teknologi informasi. Melalui kerangka regulasi tersebut, OJK secara konsisten mendorong seluruh lembaga perbankan untuk terus memperkuat sistem keamanan digitalnya sekaligus meningkatkan kemampuan manajemen risiko dalam menghadapi berbagai ancaman siber yang semakin beragam. Hal ini mempertegas bahwa kehadiran dan pengawasan dari pihak regulator merupakan salah satu faktor kunci yang tidak bisa dipisahkan dari upaya menjaga ketahanan dan keamanan sistem perbankan di tengah derasnya arus digitalisasi layanan keuangan.

Statistik Serangan Siber di Sektor Keuangan Indonesia

Tahun	Jumlah Insiden Siber (Indonesia)	Kerugian Global Sektor Keuangan	Catatan Penting
2021	~1,6 miliar anomali lalu lintas siber (BSSN)	USD 17,5 miliar	Lonjakan insiden akibat peningkatan digital banking masa pandemi
2022	~370 juta insiden terdeteksi (BSSN)	USD 18,3 miliar	BI menjadi korban ransomware Conti; 44 GB data terekspos
2023	~361 juta insiden (BSSN); sektor keuangan target utama	USD 22,0 miliar (est.)	BSI menjadi korban LockBit 3.0; insiden terbesar di perbankan RI
2024	~330,5 juta insiden (BSSN); PDNS terdampak ransomware	USD 25,0 miliar (est.)	BSSN: sektor keuangan masih masuk 3 sektor tersering diserang

Kasus serangan ransomware yang menimpa Bank Syariah Indonesia semakin mempertegas kenyataan bahwa ancaman keamanan siber di sektor keuangan terus mengalami eskalasi yang mengkhawatirkan. Merujuk pada data yang tersedia, jumlah serangan siber yang tercatat di Indonesia mencapai angka sekitar 361 juta kasus sepanjang tahun 2023. Angka tersebut menempatkan Indonesia sebagai salah satu negara dengan tingkat kerawanan siber yang masih tergolong tinggi. Memasuki tahun 2024, jumlah serangan yang berhasil terdeteksi pun masih berada pada level yang cukup mengintimidasi, yakni berkisar di angka 330,5 juta kasus. Tren ini secara jelas menggambarkan bahwa ancaman kejahatan siber terus bertumbuh dan berevolusi seiring dengan semakin masifnya pemanfaatan teknologi digital di berbagai sektor kehidupan, termasuk di dalamnya sektor perbankan dan industri jasa keuangan secara keseluruhan. Sektor keuangan memang kerap menjadi incaran utama para pelaku kejahatan siber, dan hal itu bukan tanpa alasan. Lembaga perbankan menyimpan begitu banyak data sensitif sekaligus mengelola arus transaksi keuangan dalam volume yang sangat besar setiap harinya, sehingga menjadikannya target yang sangat menggiurkan bagi para peretas. Oleh sebab itu, sudah menjadi keharusan bagi setiap lembaga perbankan untuk terus berkomitmen dalam memperkuat dan memutakhirkan sistem keamanan teknologi informasinya, agar data nasabah tetap terlindungi dengan baik dan kepercayaan masyarakat terhadap layanan perbankan digital dapat senantiasa terjaga.

KESIMPULAN

Berdasarkan seluruh pembahasan yang telah diuraikan sebelumnya, dapat ditarik kesimpulan bahwa kemajuan teknologi digital di sektor perbankan memang membawa sejumlah kemudahan yang nyata dalam berbagai aspek layanan keuangan, namun di sisi lain juga turut memperbesar potensi risiko terhadap ancaman keamanan siber yang tidak bisa dianggap remeh. Kasus serangan ransomware yang dialami oleh Bank Syariah Indonesia pada tahun 2023 menjadi bukti konkret bahwa sistem perbankan digital yang ada saat ini masih

menyimpan celah-celah kerentanan yang sewaktu-waktu dapat dieksploitasi oleh pihak-pihak yang tidak bertanggung jawab. Gangguan layanan perbankan yang timbul akibat serangan tersebut dampaknya tidak hanya dirasakan pada tataran operasional bank semata, melainkan juga berpotensi mengikis kepercayaan masyarakat secara lebih luas terhadap keamanan dan keandalan layanan perbankan berbasis digital. Dalam menghadapi ancaman yang terus berkembang tersebut, kehadiran Otoritas Jasa Keuangan sebagai lembaga pengawas memegang peranan yang sangat strategis, yakni dalam memastikan bahwa setiap lembaga perbankan telah menerapkan sistem keamanan teknologi informasi yang benar-benar memadai dan sesuai dengan standar yang ditetapkan. Melalui penerbitan regulasi yang tepat sasaran serta pelaksanaan pengawasan yang konsisten dan menyeluruh, diharapkan industri perbankan nasional dapat semakin meningkatkan kesiapan dan ketangguhannya dalam menghadapi berbagai bentuk risiko keamanan siber yang terus mengalami perkembangan dari waktu ke waktu.

Saran

Ke depannya, pihak perbankan diharapkan tidak berhenti berbenah dalam hal penguatan sistem keamanan teknologi informasi yang dimiliki, sekaligus terus mempermatang manajemen risiko yang berkaitan dengan ancaman siber. Tidak cukup sampai di situ, evaluasi menyeluruh terhadap sistem keamanan yang ada juga perlu dilaksanakan secara rutin dan berkala, sehingga setiap potensi kelemahan atau celah kerentanan yang mungkin ada dapat segera teridentifikasi dan ditangani sebelum sempat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Sementara itu, bagi OJK selaku regulator, diharapkan fungsi pengawasan yang diembannya dapat terus diperkuat dan dipertegas, termasuk dengan menyediakan pedoman yang lebih rinci dan aplikatif terkait standar penerapan keamanan siber di lingkungan perbankan. Dengan terjalinnya sinergi dan kerja sama yang solid antara regulator dan seluruh lembaga perbankan, diharapkan risiko serangan siber dapat ditekan serendah mungkin, sehingga stabilitas sistem keuangan nasional tetap dapat terjaga dengan baik dalam jangka panjang.

DAFTAR PUSTAKA

Kasmir. (2019). Manajemen Perbankan. Jakarta: PT Raja Grafindo Persada.

Keuangan, O. J. (2022). Peraturan OJK tentang Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum. Jakarta: OJK.

Keuangan, O. J. (2023). Statistik Perbankan Indonesia. Jakarta: OJK.

Nugroho, Y. (2021). Keamanan sistem informasi dalam menghadapi ancaman kejahatan siber. Jurnal Informatika, 10(1), 15–24.

Rahmawati, D. &. (2021). Penerapan manajemen risiko teknologi informasi pada industri perbankan. Jurnal Sistem Informasi, 17(1), 45–56.

Sari, M. &. (2022). Analisis risiko keamanan siber pada sektor perbankan di Indonesia. Jurnal Ekonomi dan Bisnis, 15(2), 120–130.

Setiawan, A. (2022). Dampak serangan siber terhadap stabilitas sektor keuangan. Jurnal Ekonomi Digital, 4(2), 60–72.

Susanto, H. &. (2020). Analisis ancaman ransomware terhadap keamanan sistem informasi. Jurnal Teknologi Informasi, 8(2), 85–94.

Tbk, P. B. (2023). Annual Report 2023. Jakarta: Bank Syariah Indonesia