STRATEGI BANK SYARIAH INDONESIA DALAM MENGATASI ANCAMAN CYBER

(Studi Kasus Kantor Cabang Pejanggik I Mataram)

SKRIPSI

Untuk Memenuhi Persyaratan
Memperoleh Gelar Sarjana (S1)

Oleh:

BAIQ LEONYTA HAYANU
NIM.2020B1C034

PROGRAM STUDI ADMINISTRASI BISNIS
KONSENTRASI PERBANKAN

FAKULTAS ILMU SOSIAL DAN ILMU POLITIK
UNIVERSITAS MUHAMMADIYAH MATARAM

2024

STRATEGI BANK SYARIAH INDONESIA DALAM MENGATASI ANCAMAN CYBER

Baiq Leonyta Hayanu[1*], Sulhan Hadi [2], Iwan Tanjung[3]

ABSTRAK

Tujuan Penelitian ini adalah untuk menganalisis Strategi Bank Syariah Indonesia Dalam Mengatasi Ancaman Cyber. Metode penelitian yang digunakan pada penelitian ini adalah kualitatif deskriptif dengan metode pengumpulan data observasi, wawancara dan dokumentasi. Pelaksanaan proses pencegahan terjadinya ancaman cyber dalam menjaga sistem operasional pada Bank Syariah Indonesia Kantor Cabang Pejanggik I Mataram merupakan kemampuan semua pihak bank baik pemimpin, pegawai, dan karyawan bank serta nasabah dalam menghadapi ancaman cyber yang terjadi dengan baik dan efisien supaya tidak terjadi hal-hal yang diinginkan selanjutnya. Proses pencegahan ancaman cyber tersebut yaitu dapat digambarkan sebagai berikut: 1) Mengembangkan strategi alternatif dan memilih strategi yang spesifik untuk diterapkan. Bank Syariah Indonesia Kantor Cabang Pejanggik I Mataram sudah menjalani strategi alternatif dalam mengukur kinerja perusahaan untuk memastikan tercapainya keputusan-keputusan yang sudah disepakati dan dapat meningkatkan kinerja setelah permasalahan terjadi. 2) Eksekusi strategi memobilisasi orang-orang dalam organisasi untuk menerapkan strategi yang dikembangkan. Bank Syariah Indonesia Kantor Cabang Pejanggik I Mataram telah memberikan edukasi kepada karyawan dan nasabah serta selalu memantau pola perubahan serangan hacker, dimana hal itu bisa membantu perusahaan menyesuaikan strategi yang ada. 3) Evaluasi strategi. Bank Syariah Indonesia Kantor Cabang Pejanggik I Mataram telah meni njau faktor eksternal dan internal pengaruh terjadinya ancaman cyber, mengukur keberhasilan strategi, serta mengambil tindakan dalam perbaikan setelah ancaman cyber tersebut terjadi dan sistem mulai pulih.

Kata Kunci: Ancaman Cyber, Bank Syariah Indonesia, Strategi

STRATEGIES OF INDONESIAN ISLAMIC BANKS IN OVERCOMING CYBER THREATS

Baiq Leonyta Hayanu[1], Sulhan Hadi [2], Iwan Tanjung[3]*

STRATEGIES OF INDONESIAN ISLAMIC BANKS IN OVERCOMING CYBER THREATS

ABSTRACT

This research aims to analyze the strategy of Indonesian Islamic banks in overcoming cyber threats. This research employs a descriptive-qualitative method, collecting data through observation, interviews, and documentation. Implementing the cyber threat prevention process is critical for maintaining the operational system at the Bank Syariah Indonesia Pejanggik I Mataram Branch Office. This process enables all bank parties, including leaders, employees, and customers, to respond appropriately and efficiently to cyber threats, thereby preventing unwanted outcomes. Here is a description of the cyber threat prevention process: 1) Develop alternative strategies and select specific strategies to implement. The Bank Syariah Indonesia Pejanggik I Mataram Branch Office has implemented alternative strategies to measure company performance, ensuring the achievement of agreed decisions and enhancing performance after problems arise. 2) Strategy execution mobilizes people in the organization to implement the developed strategy. The Bank Syariah Indonesia Pejanggik I Mataram Branch Office has provided education to employees and customers, and it continuously monitors changing patterns of hacker attacks, which can help companies adjust existing strategies. 3) Evaluating the strategy. Bank Syariah Indonesia Pejanggik I Mataram Branch Office has reviewed external and internal factors influencing the occurrence of cyber threats, measuring the strategy's success, and taking action for improvement after the cyber threat occurred and the system began to recover.

Keywords: Cyber Threat, Bank Syariah Indonesia, Strategy.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Bank merupakan lembaga keuangan yang bekerja berdasarkan kepercayaan terhadap masyarakat. Selama beroperasi, bank mengumpulkan uang dari masyarakat umum serta mendistribusikannya kembali kepada masyarakat umum, dan didistribusikan dalam bentuk kredit kepada masyarakat. Menurut pasal 1 ayat 11 Undang-Undang Republik Indonesia Nomor 10 Tahun 1998 tentang Perbankkan, yang menyatakan bahwa "Kredit adalah penyediaan uang atau tagihan yang dapat dipersamakan dengan itu, berdasarkan persetujuan atau kesepakatan pinjam-meminjam antara bank dengan pihak lain yang mewajibkan pihak peminjam untuk melunasi utangnya setelah jangka waktu tertentu dengan pemberian bunga".

Sesuai dengan Undang-Undang Nomor 21 Tahun 2008, "Perbankan Syariah adalah segala sesuatu yang menyangkut tentang Bank Syariah dan Unit Usaha Syariah, mencakup kelembagaan, kegiatan usaha, serta cara dan proses dalam melaksanakan kegiatan usahanya". Yang dimaksud dengan Perbankan Syariah dalam Pasal 1 Ayat 7, "Bank Syariah adalah Bank yang menjalankan kegiatan usahanya berdasarkan Prinsip Syariah dan menurut jenisnya terdiri atas Bank Umum Syariah dan Bank Pembiayaan Rakyat Syariah."

Bank menawarkan layanan perbankan untuk transaksi keuangan terutama untuk membuat transaksi lebih nyaman bagi nasabah. Layanan ATM dan BSI Mobile (Mbanking Bank Syariah Indonesia) tersedia selain pelayanan yang ditawarkan oleh kantor cabang.

Internet banking muncul sejak tahun 1998 di Indonesia. Sebuah bank swasta nasional memulai penggunaan *internet banking* pada tahun tersebut. Karena efektivitas dan fleksibilitasnya, *internet banking* menjadi semakin populer di Indonesia dari waktu ke waktu. Namun, jika dibandingkan dengan opsi lain, *internet banking* dapat menawarkan alternatif dalam menghemat penggunaan biaya operasional *(cost effective)* dengan meminimalkan biaya transaksi serendah mungkin hingga 79% jika dibandingkan dengan lainnya.(Faridatul Khusnul Khotimah, 2022)

Dari banyaknya manfaat, peningkatan keuntungan serta inklusi keuangan yang didapat dari layanan digital ini, ada sejumlah risiko yang juga bisa muncul. Risiko-risiko ini termasuk kemungkinan serangan siber dan juga kegagalan sistem, yang dapat membahayakan kemampuan sektor keuangan untuk menggunakan teknologi. Risiko siber merupakan risiko operasional dimana aset teknologi dan informasi dapat berdampak pada kerahasiaan, ketersediaan, dan integritas data atau sistem data. Selain itu, jika risiko siber tersebut terjadi, hal ini dapat mempengaruhi bank dan nasabah. Apabila dilihat dari skala yang lebih luas, risiko siber juga dapat berdampak terhadap instabilitas sistem keuangan.(Faridatul Khusnul Khotimah, 2022)

Menurut McGuire, Mike, dan Samantha Dowling 2013; Kejahatan dunia maya *(cybercrime)* adalah salah satu contoh nyata bagaimana teknologi memberikan dampak yang merugikan. *Cybercrime* dapat dilakukan menggunakan alat seperti komputer, jaringan komputer, atau semua jenis teknologi komunikasi informasi. (Kwarto & Angsito, 2018) Tindakan ini mencakup penyebaran virus atau *malware* lainnya, pembajakan *(Hacking)*, serta semua penolakan yang dikirim melalui serangan pada layanan yang ada dalam *software*.

Tabel Data Cyber Crime Bulan Januari-Agustus 2023

Bulan	Cyber Crime
Januari 2023	3.122
Februari 2023	5.580
Maret 2023	5.977
April 2023	2.988
Mei 2023	24.958
Juni 2023	64.525
Juli 2023	2.613
Agustus 2023	28.271
Jumlah	138.034

Sumber: bssn.co.id

Dari rekapan data BSSN (Badan Siber dan Sandi Negara) pada tabel *cyber crime* di diatas dapat kita lihat bahwa dari bulan Januari-Agustus telah terjadi 138.034 kali kejahatan siber (*cyber crime*), dan *cyber crime* terendah terjadi pada bulan Juli 2023 sebanyak 2.613 kali dan paling banyak terjadi pada bulan Juni 2023 sebanyak 64.525 kali.

Dari pernyataan Mohamad Miftah selaku Direktur Penelitian yang dilakukan oleh Departemen Penelitian dan Pengaturan Perbankan OJK (Otoritas Jasa Keuangan) bahwa industri keuangan atau perbankan menduduki peringkat pertama dari terjadinya serangan *cyber*, namun disisi lain ternyata OJK (Otoritas Jasa Keuangan) sendiri sudah memiliki regulasi untuk keamanan *cyber* yaitu untuk BPR (Bank Perkreditan Rakyat) regulasi yang diberikan, mulai dari kebijakan, prosedur, wewenang dan tanggung jawab, serta ruang lingkup tentang pengoprasian teknologi informasi. Mohamad Miftah juga menyampaikan bahwa pada tahun 2022 serangan *cyber* kemungkinan akan semakin meningkat.

Tabel Data Cyber Crime Bank Syariah Indonesia

Nama	Jumlah Serangan Siber
Phising/Social Engine	**1.769**
Skimming di ATM Prima	**231**
Skimming di ATM Bersama	**63**
Jumlah	**2.063**

Sumber: katadata.co.id (Bank Syariah Inonesia, 28 April 2023)

Berdasarkan data laporan Bank Syariah Indonesia diatas, sepanjang tahun 2022 ada 2.063 ancaman kejahatan siber, namun tidak ada yang berupa serangan *resomware*. Pada tahun 2022, Bank Syariah Indonesia mendapat 1.769 upaya *phising/social engineering* terhadap nasabah. *Phising* merupakan kejahatan yang berupa pengiriman alamat website palsu yang tampilannya sangat mirip dengan website aslinya. Hal tersebut bertujuan supaya nasabah terkecoh sampai memasukkan informasi pribadi ke website palsu yang sudah dikirimkan, seperti password, username, nomor pin dan sebagainya. Adapun *social engineering* yaitu bagian dari *phising*, dimana pelaku menelpon nasabah dengan nomor asing, pesan singkat, serta media lainnya, setelah itu pelaku mengarahkan nasabah untuk membuka website tertentu untuk mencuri data serupa.

Sepanjang tahun 2022 Bank Syariah Indonesia juga menemukan 231 kasus kecurigaan *skimming* pada jaringan ATM Prima, dan 63 kasus pada jaringan ATM Bersama. *Skimming* adalah upaya pencurian data pada kartu ATM. Kejahatan ini tergolong *cyber crime* dan bisa dilakukan dengan memasang kamera tersembunyi pada mesin ATM untuk mengintip nomor pin kartu ATM nasabah. Selain itu, ada *skimming* yang dilakukan dengan memasang alat khusus pada kolom kartu mesin ATM untuk menyalin data kartu ATM nasabah secara digital.

Seperti kasus yang terjadi pada awal tahun 2023 bulan Mei telah terjadi *cyber crime* terhadap Bank Syariah Indonesia dan masalah tersebut berlangsung kurang lebih satu minggu sebelum pihak Bank Syariah Indonesia menemukan solusi terhadap permasalahan tersebut. Aplikasi *mbanking* milik Bank Syariah Indonesia (BSI) yaitu BSI Mobile tiba-tiba mengalami gangguan sejak Senin (8/5/2023) dan belum sepenuhnya pulih sampai Rabu (10/5/2023).

Tabel Data Cyber Crime Bank Syariah Indonesia

Kantor Cabang Pejanggik I

No	Kelompok Cyber	Serangan Resomware
1.	Lock Bit	115
2.	Conti	102
3.	Ryuk	56
4.	Black Cat	38
5.	Revil	48
6.	Maze	35
7.	Doppel Paymer	38
8.	Wanna Cry	48
9.	Not Petya	46
10.	Hive	32
	Jumlah	558

Sumber: Bank Syariah Indonesia Pejanggik I (16 November 2023)

Aplikasi *mobile banking* milik Bank Syariah Indonesia, yaitu BSI Mobile tidak bisa diakses selama beberapa hari pada awal bulan Mei 2023. Dari beberapa data Bank Syariah Indonesia Kantor Cabang Pejanggik I Mataram terjadi serangan dari beberapa kelompok pada tabel diatas, dimana serangan *resomware* paling banyak dilakukan dari kelompok Lock Bit sebanyak 115 kali dan paling sedikit dari kelompok Hive sebanyak 32 kali.

Pada dasarnya, *resomeware* merupakan salah satu dari jenis *malware*, yaitu perangkat lunak (*software*) yang bisa menyusup ke jaringan, sistem, atau server pada komputer serta bisa mengubah data yang ada didalamnya.

Manajemen Bank Syariah Indonesia (BSI) menyatakan mereka sedang melakukan pemeliharaan aplikasi. Namun, menurut Direktur Eksekutif ICT Intitute, Heru Sutadi, ada kemungkinan Bank Syariah Indonesia diserang oleh siber dan memungkinkan sistem dikunci, serta tidak kemungkinan terkena *rasomware*. Kasus serangan siber pada sistem aplikasi ini merupakan serangan pertama kali yang terjadi pada Bank Syariah Indonesia. Selain itu, ada kebutuhan untuk meningkatkan kesadaran dan edukasi nasabah perbankan mengenai masalah ini. Banyak peneliti telah mempelajari mitigasi risiko. Penelitian Yudi Herdiana, Zen Munawar, dan Novianti Indah Putri, misalnya, menemukan bahwa mitigasi keamanan *cyber* diperlukan untuk mencegah pencurian data dan mencegah gangguan pada sistem informasi, perangkat lunak, dan perangkat keras. Dikarenakan berlipatnya kekhawatiran, serta kemungkinan peningkatan pada serangan *cyber*, dan tentunya peningkatan yang ditimbulkan memiliki arti yang lebih luas melebihi target semacamnya.

Urgensi penelitian ini mengangkat sebuah permasalahan serangan *cyber* yang menghambat berjalannya sistem kerja yang terjadi pada Bank Syariah Indonesia Kantor Cabang Pejanggik I Mataram pada awal bulan Mei 2023, nantinya akan ditindak lanjuti permasalahan tersebut. Manfaat penelitian ini secara praktis bisa dijadikan bahan evaluasi bagi Bank Syariah Indonesia Kantor Cabang Pejanggik I Mataram dan bisa juga manfaatnya untuk kalangan akademis yaitu penelitian ini akan memberikan kontribusi terkait topik tertentu bagi kalangan akademisi. Penelitian Nida Rafa Arofah dan Yeni Priatnasari (2020) dengan judul *Internet Banking* dan *Cyber Crime*: Sebuah Studi Kasus di Perbankkan Nasional yang membahas terkait Ancaman *Cyber Crime* di Perbankan Nasional, sedangkan pembahasan yang diangkat oleh peneliti adalah Ancaman *Cyber* pada Bank Syariah Indonesia Kantor Cabang Pejanggik I Mataram. Objek penelitian ini berdasarkan survei dan pertimbangan peneliti dalam menjabarkan keunikan yang ada ditempat penelitian pada saat survei awal tepat pada bulan Mei 2023 saat melakukan magang.

Alasan peneliti melakukan penelitian ini yaitu karena pada Bank Syariah Indonesia pernah terjadi ancaman *cyber* pada bulan Mei 2023. Terlepas dari Bank Syariah Indonesia merupakan perusahaan dalam sektor keuangan serta banyaknya kemudahan yang bisa meningkatkan keuntungan dan inklusi keuangan yang didapatkan dengan adanya layanan digital, terdapat beberapa risiko yang bisa timbul dan dapat mengancam berjalanannya sistem layanan teknologi pada bidang finansial. Beberapa hal tersebut bisa menjadi awal mulanya terjadi ancaman *cyber* pada sistem layanan yang ada dan dapat berisiko tinggi untuk oprasional yang

didalamnya terdapat aset informasi dan teknologi yang mampu mempengaruhi kerahasiaan, ketersediaan dan integritas informasi yang terdapat pada sistem layanan Bank Syariah Indonesia.

Dari uraian diatas peneliti tertarik meneliti lebih lanjut terkait upaya yang dilakuakan oleh pihak perusahaan untuk menghadapi adanya ancaman *cyber* tersebut. Dan peneliti memilih untuk menarik judul "**STRATEGI BANK SYARIAH INDONESIA DALAM MENGATASI ANCAMAN CYBER (Studi Kasus Kantor Cabang Pejanggik I Mataram)"**

1.2 Rumusan Masalah

1. Bagaimanakah pengaruh ancaman *cyber* pada Bank Syariah Indonesia Kantor Cabang Pejanggik I Mataram?
2. Bagaimanakah strategi pencegahan yang bisa dilakukan Bank Syariah Indonesia Kantor Cabang Pejanggik I Mataram terhadap ancaman *cyber*?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah, maka tujuan penelitian dirumuskan sebagai berikut:

1. Untuk mengetahui bagaimanakah pengaruh ancaman *cyber* pada Bank Syariah Indonesia Kantor Cabang Pejanggik I Mataram.
2. Untuk mengetahui bagaimanakah strategi pencegahan yang bisa dilakukan Bank Syariah Indonesia Kantor Cabang Pejanggik I

Mataram terhadap ancaman *cyber*.

1.4 Manfaat Penelitian

Penelitian ini diharapkan dapat bermanfaat bagi berbagai pihak:

1. **Manfaat Teoritis**

   Hasil penelitian ini hendaknya membawa manfaat bagi pengembangan ilmu pengetahuan dan pemahaman khususnya dalam bidang teknologi yang berkaitan dengan perbankan.

2. **Manfaat Praktis**

   Hasil penelitian ini hendaknya dapat menambah wawasan dan pengetahuan tentang apa saja yang menyebabkan terjadinya ancaman *cyber* pada Bank Syariah Indonesia Kantor Cabang Pejanggik I Mataram.

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan pembahasan yang dipaparkan pada bab sebelumnya mengenai Strategi Bank Syariah Indonesia Kantor Cabang Pejanggik I Mataram dalam Mengatasi Ancaman Cyber, maka dapat disimpulkan bahwa:

5.1.1 Pengaruh Ancaman Cyber

Terjadinya serangan *cyber* pada Bank Syariah Indonesia Kantor Cabang Pejanggik I Mataram yang dimana hal ini terjadi karena faktor eksternal seperti serangan resomeware dimana resomeware merupakan istilah yang mencakup jenis malware tertentu yang melakukan serangan terhadap suatu sistem komputer dengan cara mengancam akan mempublikasikan, menghapus, atau menahan akses ke data pribadi data yang penting. Karena adanya serangan *cyber* ini dapat mempengaruhi aktifitas nasabah dalam melakukan transaksi seperti pembayaran tagihan Listrik, *top up eWallet*, pembayaran *eCommerce*, hingga pembayaran zakat pada aplikasi BSI Mobile. Karena serangan *Cyber* ini aktivitas operasional pada Bank Syariah Indonesia Kantor Cabang Pejanggik I menjadi terganggu seperti kerugian matrial berupa tertundanya transaksi selama sistem mengalami gangguan sehingga Bank Syariah Indonesia harus mengeluarkan dana darurat untuk melakukan *inciden handling* hal ini juga menyebabkan berkurangnya tingkat kepercayaan nasabah.

5.1.2 Strategi Pencegahan Ancaman Cyber

Pelaksanaan proses pencegahan terjadinya ancaman *cyber* dalam menjaga sistem operasional pada Bank Syariah Indonesia Kantor Cabang Pejanggik I Mataram merupakan kemampuan semua pihak bank baik pemimpin, pegawai, dan karyawan bank serta nasabah dalam menghadapi ancaman *cyber* yang terjadi dengan baik dan efisien supaya tidak terjadi hal-hal yang diinginkan selanjutnya. Proses pencegahan ancaman cyber tersebut yaitu dapat digambarkan sebagai berikut:

1) Mengembangkan strategi alternatif dan memilih strategi yang spesifik untuk diterapkan. Bank Syariah Indonesia Kantor Cabang Pejanggik I Mataram sudah menjalani strategi alternatif dalam mengukur kinerja perusahaan untuk memastikan tercapainya keputusan-keputusan yang sudah disepakati dan dapat meningkatkan kinerja setelah permasalahan terjadi.
2) Eksekusi strategi memobilisasi orang-orang dalam organisasi untuk menerapkan strategi yang dikembangkan. Bank Syariah Indonesia Kantor Cabang Pejanggik I Mataram telah memberikan edukasi kepada karyawan dan nasabah serta selalu memantau pola perbahan serangan hacker, dimana hal itu bisa membantu perusahaan menyesuaikan strategi yang ada.
3) Evaluasi strategi. Bank Syariah Indonesia Kantor Cabang Pejanggik I Mataram telah meninjau faktor eksternal dan internal pengaruh

terjadinya ancaman cyber, mengukur keberhasilan strategi, serta mengambil tindakan dalam perbaikan setelah ancaman cyber tersebut terjadi dan sistem mulai pulih.

5.2 Saran

Dari berbagai permasalahan yang diuraikan di atas, maka penulis ingin menyampaikan saran:

5.2.1 Kepada Bank Syariah Indonesia Kantor Cabang Pejanggik I Mataram

Diharapkan agar semakin aktif dalam menerapkan keamanan sistem (*cyber security)* untuk meminimalisir terjadinya ancaman cyber pada oprasional perusahaan serta pengawasan ekstra terhadap *resomeware* yang dapat merugikan.

5.2.2 Bagi Peneliti

Hasil penelitian ini dapat digunakan sebagai bahan pelajaran tentang Strategi Bank Syariah Indonesia dalam Mengatasi Ancaman *Cyber* serta agar dapat melakukan kajian yang lebih dalam lagi mengenai Strategi Mengatasi Ancaman *Cyber.*