BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Sektor perbankan adalah elemen penting dalam struktur perekonomian suatu negara. Peran utama perbankan adalah menghubungkan individu atau lembaga yang memiliki dan adengan mereka yang memerlukan, yang deikenal sebgai intermediasi keuangan. Keberadaan bank sangat krusial bagi keamjuan ekonomi suatu Negara (Fitri, 2021). Saat ini, jaringan internet telah menjadi alat yang banyak digunakan dalam dunia bisnis, baik di tingkat lokal maupun global. Pemanfaatan internet mencakup berbagai aspek bisnis, mulai dari pengumpulan data untuk proses rekrutmen hingga pengembangan strategi pemasaran, yang telah menjadi praktik umum. Keberadaan internet memberikan manfaat yang besar dan signifikan bagi komunitas bisnis (Syahputra, 2020). Internet telah menciptakan peluang baru bagi perusahaan kecil dan besar untuk beroperasi secara eksklusif dalam ranah online. Bisnis online mengacu pada model usaha yang sepenuhnya bergantung pada internet sebagai saluran utama untuk memasarkan dan menjual produk atau layanan mereka.

Salah satu fitur dalam layanan perbankan elektronik yang sering digunakan adalah ATM, phone banking, dan internet banking. Fasilitas-fasilitas ini telah mengubah cara pelayanan dari metode manual menjadi berbasis teknologi

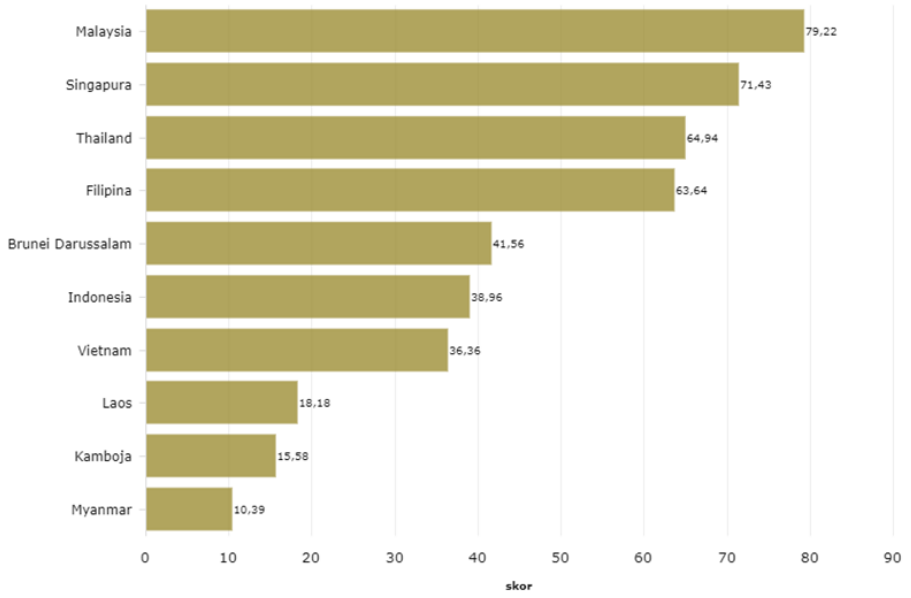
Namun, dengan perkembangan teknologi yang pesat, pengguna tidak luput dari risiko negatif seperti serangan kejahatan melalui internet yang dapat mengancam keamanan mereka. Beberapa nasabah juga bisa menjadi korban kejahatan yang dilakukan oleh pelaku di media sosial, yang dikenal sebagai *cybercrime*.(Sari, 2022).

Kemajuan teknologi digital dan internet telah mengubah cara kita berinteraksi dengan dunia, termasuk dalam transaksi keuangan. Nasabah bank syariah semakin memanfaatkan layanan perbankan digital untuk melakukan berbagai transaksi, seperti transfer dana, pembayaran tagihan, dan pengelolaan rekening. Namun, seiring dengan kemajuan ini, serangan *cybercrime* juga semakin meningkat dengan metode yang semakin canggih. Menurut Ikawati (2012) *cybercrime* dapat diartikan sebagai tindakan kriminal di mana komputer digunakan sebagai alat utama. *cybercrime* mengacu pada kejahatan yang dilakukan melalui komputer atau jaringan elektronik, termasuk serangan terhadap sistem perbankan online dan pencurian data pribadi nasabah. Menurut Kwarto & Angsito (2018) Tindakan ini mencakup penyebaran virus atau *malware* lainnya, pembajakan (*hacking*), dan serangan *denial-of-service* (DoS) yang mengganggu layanan dalam perangkat lunak.

Dengan kemajuan teknologi komunikasi dan informasi, jenis serangan di dunia maya menjadi semakin kompleks. Sebelumnya, istilah *hacker* dan *cracker* merujuk pada individu dengan kemampuan khusus yang memasuki sistem komputer untuk berbagai tujuan. Saat ini, banyak mesin atau sistem telah

dikembangkan untuk melakukan teknik penyusupan yang dapat merusak sistem yang ditargetkan. (Sari, 2022)

Gambar 1. 1 Indeks Keamanan Siber Negara-Negara Asia Tenggara



Sumber : databoks.katadata.co.id

Menurut pada Gambar 1.1 data *National Cyber Security Index* (NCSI) yang dikutip pada Senin (7/3), Keamanan siber Indonesia berada di peringkat ke-6 di Asia Tenggara dan peringkat ke-83 dari 160 negara secara global. Penilaian ini dilakukan oleh NCSI berdasarkan sejumlah indikator, termasuk peraturan hukum terkait keamanan siber, keberadaan lembaga pemerintah yang menangani keamanan siber, kerja sama pemerintah dalam bidang tersebut, serta bukti-bukti publik seperti situs resmi pemerintah atau program terkait lainnya. Berdasarkan indikator-indikator ini, NCSI memberikan skor 38,96 dari 100 untuk keamanan

siber Indonesia. Skor ini jauh di bawah negara-negara tetangga dan menempatkan Indonesia di peringkat ke-3 terendah di antara negara-negara G20. (Dihni, 2022).

Menurut databoks.katadata.co.id, pada tahun 2022 BSI mendeteksi 1.767 upaya phishing/social engineering terhadap nasabahnya. Phishing adalah bentuk kejahatan siber di mana alamat website palsu dikirimkan kepada nasabah, dengan tampilan yang sangat mirip dengan website asli. Tujuannya adalah untuk menipu nasabah agar memasukkan informasi pribadi mereka ke website palsu tersebut, seperti nama akun (*username*), kata sandi (*password*), nomor PIN, dan sebagainya. Social engineering adalah bagian dari phishing, di mana pelaku menghubungi nasabah melalui telepon, pesan singkat, atau media lain, dan mengarahkan mereka untuk membuka website tertentu dengan tujuan mencuri data serupa.

Sepanjang tahun 2022, BSI juga menemukan 232 kasus dugaan skimming di jaringan ATM Prima dan 64 kasus di jaringan ATM Bersama. Skimming adalah upaya pencurian data kartu ATM yang termasuk dalam kategori kejahatan siber. Kejahatan ini dapat dilakukan dengan memasang kamera tersembunyi di mesin ATM untuk mengintip nomor PIN kartu ATM nasabah. Selain itu, skimming juga dapat dilakukan dengan memasang alat khusus di slot kartu mesin ATM untuk menyalin data kartu ATM nasabah secara digital (Ahdiat, 2023).

Dilansir tribunjogja.com, pada awal bulan Mei 2023, nasabah BSI mulai mengalami gangguan pelayanan dari tanggal 8 hingga 11 Mei 2023. Gangguan tersebut meliputi kesulitan akses ke BSI Mobile, ATM, dan transaksi di kantor cabang. Kabar terbaru mengungkapkan bahwa gangguan tersebut disebabkan oleh

aktivitas peretasan. Dilansir kompas.tv, kelompok peretas ransomware, LockBit, meminta tebusan sebesar 20 juta dolar AS atau setara dengan Rp295 miliar. BSI menawar dengan harga 100.000 dolar AS. Namun, LockBit menolak dan tetap mempertahankan jumlahnya, yaitu 20 juta dolar AS. BSI menganggap jumlah tersebut terlalu besar, dan meminta LockBit untuk memberikan satu contoh nama pengguna dan kata sandi yang mereka curi untuk diverifikasi keasliannya. Kemudian dilansir wartakota.tribunnews.com Ancaman dari LockBit tidak hanya berupa ancaman kosong. Kelompok peretas ini benar-benar telah menyebarkan data yang dicuri dari Bank Syariah Indonesia (BSI) ke dark web. LockBit mengancam akan mempublikasikan data tersebut jika BSI tidak membayar tebusan hingga 16 Mei atau dalam waktu 72 jam setelah mengumumkan serangan cyber kepada publik. BSI menanggapi hal tersebut dengan menegaskan bahwa data dan dana nasabah tetap dalam keadaan aman, sehingga nasabah dapat melakukan transaksi dengan normal dan tanpa risiko.

Dari adanya kasus-kasus tersebut tentunya berhubungan dengan *cyber security*. Menurut Wulansari (2020) Perlindungan data pribadi adalah sistem aturan yang menyeluruh untuk mengatur individu, lembaga hukum, dan organisasi lainnya dalam undang-undang khusus yang mengatur tentang penggunaan data pribadi. Konsep ini secara keseluruhan terkait dengan aspek keamanan. Sedangkan, menurut Adiyanti (2014) *cyber security* adalah kumpulan alat, konsep, perlindungan, pedoman, strategi manajemen risiko, tindakan, pelatihan, praktik

terbaik, jaminan, dan teknologi yang digunakan untuk melindungi lingkungan dari kejahatan serta melindungi organisasi dan aset pengguna.

Keamanan yang rendah dapat mengakibatkan kerugian finansial bagi nasabah dan merusak reputasi serta kepercayaan terhadap lembaga keuangan terkait. Nasabah yang menjadi korban serangan cybercrime mungkin kehilangan kepercayaan terhadap bank tersebut dan cenderung mencari bank lain yang menawarkan sistem keamanan yang lebih baik. Dampak dari serangan cybercrime tidak hanya berdampak finansial, tetapi juga dapat memiliki dampak psikologis bagi nasabah yang merasa privasi dan keamanan dalam transaksi perbankan mereka terganggu. Hal ini dapat mengurangi loyalitas nasabah dan bahkan mendorong mereka untuk mencari alternatif di luar industri perbankan yang dianggap lebih aman. Jika bank mampu menjamin keamanan data dan transaksi baik secara offline maupun online melalui layanan teller, mesin ATM, dan mobile banking, maka rasa aman dan loyalitas nasabah akan meningkat. Menurut Handoko & Ronny (2021) rasa aman adalah saat pelanggan merasa nyaman menggunakan produk dan layanan yang disediakan oleh bank.

Bedasarkan penelitian terdahulu yang dilakukan oleh Fitri (2021) Penelitian menunjukkan bahwa internet banking memiliki dampak positif dan signifikan terhadap kepercayaan nasabah, sementara cyber crime memiliki dampak negatif dan signifikan terhadap kepercayaan nasabah. Selain itu, kepercayaan nasabah terhadap internet banking dan cyber crime secara bersamaan memiliki dampak positif dan negatif yang signifikan terhadap kepercayaan

nasabah. Penelitian yang dilakukan oleh Sari (2023) hasil penelitian menunjukkan bahwa secara spesifik, variabel Cybercrime berpengaruh terhadap kepercayaan nasabah di Bank Syariah Indonesia Banjarbaru A Yani. Hal ini terbukti dari nilai t hitung sebesar 4,158 dengan tingkat signifikansi sebesar 0,000. Sedangkan penelitian yang dilakukan oleh Ikawati (2012) hasil perhitungan dengan menggunakan SPSS versi 16 diketahui bahwa reputasi perusahaan dan kepercayaan berpengaruh secara simultan terhadap loyalitas nasabah. Di penelitian Kwarto & Angsito (2018) Hasil menunjukan bahwa pengaruh *hacking* secara empiris terhadap *cyber security compliance* di sektor keuangan, pengaruh phising secara empiris terhadap *cyber security compliance* di sektor keuangan, dan pengaruh malware secara empiris terhadap *cyber security compliance* di sektor keuangan.

Berdasarkan uraian tersebut, peneliti memiliki ketertarikan untuk melakukan penelitian yang mengenai loyalitas nasabah Bank BSI yang dipengaruhi persepsi seperti *Cybercrime* dan *Cyber SecurityI*. Dengan demikian penulis melakukan penelitian dengan judul penelitian **"Pengaruh *Cybercrime* dan *Cyber Security* Terhadap Loyalitas Nasabah Bank Syariah Indonesia Di Yogyakarta"**

B. Rumusan Masalah

Berdasarkan masalah di atas, maka penelitian ini mempunyai rumusan masalah sebagai berikut:

1. Apakah *cybercrime* secara parsial berpengaruh terhadap loyalitas nasabah Bank BSI di Yogyakarta?
2. Apakah *cyber security* secara parsial berpengaruh terhadap loyalitas nasabah Bank BSI di Yogyakarta
3. Apakah *cybercrime* dan *cybersecurity* secara simultan berpengaruh terhadap loyalitas nasabah Bank BSI di Yogyakarta

C. Tujuan Masalah

Bedasarkan rumusan masalah di atas, maka peneliti memiliki tujuan masalah sebagai berikut:

1. Untuk mengetahui pengaruh *cybercrime* terhadap loyalitas nasabah Bank Syariah Indonesia di Yogyakarta
2. Untuk mengetahui pengaruh *cybersecurity* terhadap loyalitas nasabah Bank Syariah Indonesia di Yogyakarta
3. Untuk mengetahui pengaruh *cybercrime* dan *cybersecurity* terhadap nasabah Bank Syariah Indonesia di Yogyakarta

D. Manfaat Penelitian

Berdasarkan rumusan masalah diatas, maka peneliti memiliki manfaat masalah sebagai berikut :

1. Manfaat Teoritis

   Untuk dapat menambah pengetahuan serta wawasan tentang terhadap perkembangan ilmu pengetahuan khususnya dibidang Perbankan Syariah mengenai Pengaruh *Cybercrime* dan *Cyber Security* terhadap Loyalitas Nasabah di Perbankan Syariah

2. Manfaat Praktis

   Hasil penelitian ini diharapkan dapat bermanfaat bagi penulis dan dapat bermanfaat bagi nasabah yang aktif menggunakan *e-banking* agar dapat memahami tentang bahaya *Cybercrime*, dan dapat menjadi masukan sekaligus pertimbangan pihak perbankan agar lebih memperhatikan dan meningkatkankan keamanan siber.

E. Sistematika Penulisan

Sistematika penulisan ini memuat lima bagian yaitu:

BAB I PENDAHULUAN

Pada bab I meliputi latar belakang masalah, rumusan masalah, tujuan masalah, manfaat penelitian, dan sistematika penulisan..

BAB II LANDASAN TEORI

BePada bab II meliputi landasan teori (*cybercrime*, *cybersecurity*, loyalitas, nasabah, bank syariah), kajian pustaka, kerangka pemikiran, pengembangan hipotesis.

BAB III METODE PENELITIAN

Pada Bab III ini dijelaskan mengenai desain penelitian, metode pengumpulan data, instrument penelitian, metode analisis data, pengujian hipotesis.

BAB IV HASIL PENELITIAN

Pada Bab IV Berisi Deskripsi Hasil Penelitian Analisis Data dan Pembahasan

BAB V PENUTUP

Pada Bab V Berisi Kesimpulan hasil penelitian dan Saran hasil penelitian