SKRIPSI

DAMPAK HOAX TERKAIT ISU SERANGAN VIRUS RANSOMWARE TERHADAP KEPERCAYAAN NASABAH DALAM PENYIMPANAN DANA DI BSI KCP BARRU

OLEH

NUR AZIZAH
2020203861206013

PROGRAM STUDI PERBANKAN SYARIAH
FAKULTAS EKONOMI BISNIS ISLAM
INSTITUT AGAMA ISLAM NEGERI PAREPARE

2024

DAMPAK HOAX TERKAIT ISU SERANGAN VIRUS RANSOMWARE TERHADAP KEPERCAYAAN NASABAH DALAM PENYIMPANAN DANA DI BSI KCP BARRU

OLEH

NUR AZIZAH
2020203861206013

Skripsi sebagai salah satu syarat untuk memperoleh gelar Sarjana Ekonomi (S.E) pada Program Studi Perbankan Syariah
Fakultas Ekonomi dan Bisnis Islam
Institut Agama Islam Negeri Parepare

PROGRAM STUDI PERBANKAN SYARIAH
FAKULTAS EKONOMI BISNIS ISLAM
INSTITUT AGAMA ISLAM NEGERI PAREPARE

2024

PERSETUJUAN KOMISI PEMBIMBING

Judul Skripsi	:	Dampak Hoax Terkait Isu Serangan Virus Ransomware Terhadap Kepercayaan Nasabah Dalam Penyimpanan Dana Di BSI Kcp Barru
Nama Mahasiswa	:	Nur Azizah
Nomor Induk Mahasiswa	:	2020203861206013
Program Studi	:	Perbankan Syariah
Fakultas	:	Ekonomi dan Bisnis Islam
Dasar Penetapan Pembimbing	:	Surat Penetapan Pembimbing Skripsi Fakultas Ekonomi dan Bisnis Islam Nomor B.5142/In.39/FEBI.04/PP.00.9/08/2023

Disetujui oleh

Pembimbing Utama	: Dr. And Bahri S. M.E., M.Fil.I.	(.....)
NIP	:197811012009121003	
Pembimbing Pendamping	: Dr. Musmulyadi, S.HI., M.M.	(.....)
NIP	: 199103072019031009	

Mengetahui :
Dekan,
Fakultas Ekonomi dan Bisnis Islam

Dr. Muzdalifah Muhammadun, M.Ag.
NIP. 19710208 200112 2 002

PENGESAHAN KOMISI PENGUJI

Judul Skripsi	: Dampak Hoax Terkait Isu Serangan Virus Ransomware Terhadap Kepercayaan Nasabah Dalam Penyimpanan Dana Di BSI Kcp Barru
Nama Mahasiswa	: Nur Azizah
Nomor Induk Mahasiswa	: 2020203861206013
Fakultas	: Ekonomi Dan Bisnis Islam
Program Studi	: Perbankan Syariah
Dasar Penetapan Pembimbing	: Surat Penetapan Pembimbing Skripsi Fakultas Ekonomi dan Bisnis Islam Nomor B.5142/In.39/FEBI.04/PP.00.9/08/2023
Tanggal Kelulusan	: 30 Juli 2024

Disahkan oleh Komisi Penguji

Dr. Andi Bahri S. M.E., M.Fil.I.	(Ketua)	(.....)
Dr. Musmulyadi, S.HI., M.M.	(Sekretaris)	(.....)
Dr. Damirah, S.E., M.M.	(Anggota)	(.....)
Sahrani, S.Si., M.E., AWP.	(Anggota)	(.....)

Mengetahui:

Dekan,

Fakultas Ekonomi dan Bisnis Islam

Dr. Muzdalifah Muhammadun, M.Ag.

NIP 19710208 200112 2 002

KATA PENGANTAR

بِسْـــــــــــــمِ اللهِ الـرَّحْمَنِ الرَّحِيْمِ

Alhamdulillah, segala puji dan syukur kepada Allah SWT atas rahmat, taufiq, hidayah, dan inayah-Nya, penulis dapat menyelesaikan tulisan ini sebagai salah satu syarat untuk meraih gelar "Sarjana Ekonomi" di Institut Agama Islam Negeri Parepare. Semoga shalawat dan salam selalu tercurah kepada Nabi Muhammad SAW, Rasul pilihan yang membawa cahaya ilmu pengetahuan. Doa juga dipanjatkan untuk keluarga, sahabat, dan seluruh pengikutnya yang setia hingga akhir zaman.

Penulis mengucapkan rasa terima kasih yang mendalam kepada Almh. Ibu kandung tercinta saya (Mamminasa), Ibunda (Nanna Bandu) dan Ayah (Abd. Hafid) tercinta atas bimbingan serta doa tulus mereka, yang telah memudahkan penulis dalam menyelesaikan tugas akademik tepat waktu.

Penulis mengucapkan terima kasih yang tulus kepada bapak Dr. Andi Bahri S. M.E., M.Fil.I. dan bapak Dr. Musmulyadi, S.HI., M.M. atas bimbingan dan bantuan yang telah mereka berikan sebagai pembimbing I dan pembimbing II. Dukungan mereka sangat berharga bagi penulis.

Selanjutnya, penulis juga menyampaikan terima kasih kepada:

1. Bapak Prof. Dr. Hannani, M.Ag. sebagai Rektor IAIN Parepare yang telah bekerja keras mengelola pendidikan di IAIN Parepare.
2. Ibu Dr. Muzdalifah Muhammadun, M.Ag. sebagai Dekan Fakultas Ekonomi dan Bisnis Islam atas pengabdiannya dalam menciptakan suasana pendidikan yang positif bagi mahasiswa.
3. Bapak I Nyoman Budiono, S.E., M.M. sebagai ketua program studi Perbankan Syariah yang telah berjasa dan mendedikasikan hidup beliau sehingga tercipta suasana pendidikan syariah saat ini yang telah berkembang dengan baik.

4. Seluruh staff IAIN Parepare yang telah memberikam izin dan informasi dalam melaksanakan penelitian di IAIN Papare.
5. Bapak Fajar selaku Kepala Cabang Bank Syariah Indonesia KCP Barru beserta seluruh jajarannya yang telah mengizinkan dan memberikan data informasi terkait penelitian.
6. Kelima kakak ku yang tersayang. Kak Herman, kak Fitri, kak Andi, kak Nurul dan saudara kembar penulis, Annizah, yang selalu memberikan motivasi dan inspirasi untuk terus melangkah maju kedepan, dan menjadi *support system* terbaik bagi penulis dalam menyelesaikan tugas akhir.
7. Keluarga besar penulis, yang selalu menjadi penyemangat bagi penulis. Terima kasih atas waktu, materi, doa yang senantiasa dilangitkan, dan seluruh hal baik yang diberikan kepada penulis selama ini.
8. Teman-teman seperjuangan program studi Perbankan Syariah angkatan 2020 yang telah memberikan banyak bantuan dalam penyelesaian skripsi ini.
9. Sahabat penulis, Riska Anugrah Putri, Annisa Nabila Salsa, dan Nabila Husaini yang telah banyak membantu dan membersamai penulis dari SMP hingga sekarang. Terima kasih atas segala bantuan, waktu, *support*, dan kebaikan yang diberikan kepada penulis selama ini. *See you on top, guys*.
10. Irna, Tika Azizah Fatirah, dan Nurawalya yang selalu membersamai, menjadi teman bertukar pikiran, tempat berkeluh kesah dan memberikan dukungan penuh pada penulis hingga sekarang. Terima kasih atas segala *support* yang diberikan kepada penulis. Dan terima kasih juga kepada Ifa Nurul Ilmah, Ainun Pratiwi, Aniq Amnur, dan Nurfadillah.
11. Seluruh teman-teman KKN Reguler posko 65 tercinta (Ikki, Yusup, Ikhwan, Wati, Ilmi, cica, Nafilah, Tika, Nunung, dan Sahabi) yang selalu membantu dan support penulis dalam penyusunan skripsi ini. Terutama, Sahabi, Wati dan Kartika Rajid yang selalu memberikan waktu, *support*, membantu serta do'a untuk menyelesaikan penulisan ini.

12. Teman-teman Magang penulis, Nurul Asmi Jamal, Julianti, Veni Marzita, Nurul Auliyah, Haerunisa dan Tiara Rezky.
13. *Last but not least*, untuk Nur Azizah. Terima kasih banyak sudah mau menepikan ego dan memilih untuk kembali bangkit dan menyelesaikan semua ini. Kamu selalu berharga, tidak peduli seberapa putus asanya kamu sekarang, tetaplah mencoba bangkit. *Love* cica.

Tidak ada kata yang dapat melukiskan rasa syukur dan terima kasih kepada seluruh pihak yang telah membantu kelancaran dalam penulisan skripsi ini yang mungkin tidak dapat penulis sebutkan, semoga Allah SWT. membalas kebaikan kalian semua dan menjadikannya sebagai amal jarriyah serta senantiasa memberikan rahmat dan pahala-Nya. Aamiin.

Harapan penulis, agar karya sederhana ini bermanfaat bagi dirinya dan para pembaca secara luas. Penulis juga mengundang pembaca untuk memberikan saran yang membangun guna menyempurnakan skripsi ini. Akhir kata, penulis mengucapkan terima kasih banyak.

Parepare, 28 Mei 2024
19 Dzulqaidah 1445 H
Penulis,

Nur Azizah
NIM. 2020203861206013

PERNYATAAN KEASLIAN SKRIPSI

Mahasiswa yang bertanda tangan di bawah ini:

Nama	:	Nur Azizah
Nim	:	2020203861206013
Tempat/tanggal lahir	:	Parepare,10 Maret 2002
Program Studi	:	Perbankan Syariah
Fakultas	:	Ekonomi dan Bisnis Islam
Judul Skripsi	:	Dampak Hoax Terkait Isu Serangan Virus Ransomware Terhadap Kepercayaan Nasabah Dalam Penyimpanan Dana Di BSI Kcp Barru

Dengan sepenuh hati dan kesabaran, saya menyatakan bahwa skripsi ini sepenuhnya merupakan karya saya sendiri. Apabila di masa mendatang terbukti dan dapat dibuktikan bahwa sebagian atau seluruh skripsi ini adalah duplikat, tiruan, plagiat, atau dibuat oleh orang lain, baik sebagian maupun seluruhnya, maka skripsi dan gelar yang diperoleh karenanya akan dianggap batal demi hukum.

Parepare, 28 Mei 2024
Penyusun,

Nur Azizah
NIM. 2020203861206013

ABSTRAK

Nur Azizah. *Dampak Hoax Terkait Isu Serangan Virus Ransomware Terhadap Kepercayaan Nasabah Dalam Penyimpanan Dana Di Bsi Kcp Barru* (Dibimbing oleh Bapak Andi Bahri dan Bapak Musmulyadi.

Pada tanggal 08 mei 2023 Bank Syariah Indonesia (BSI) mengalami gangguan pada sistem ITnya di karenakan adanya serangan virus *ransomware* yang mengakibatkan nassabah tidak bisa melakukan transaksi. Oleh karena itu, penelitian ini bertujuan untuk (1) Mengetahui bentuk serangan yang diduga Virus *Ransomware* Terhadap Bank Syariah Indonesia (BSI) di Kcp Barru, (2) Mengetahui dampak serangan virus terhadap kepercayaan nasabah Bank Syariah Indonesia (BSI) di Kcp Barru, (3) Mengetahui upaya Bank Syariah Indonesia (BSI) di Kcp Barru dalam memulihkan kepercayaan nasabah setelah terjadinya serangan virus *ransomware*.

Penelitian ini menggunakan metode pendekatan kualitatif dengan jenis penelitian lapangan deskriptif dan survei. Metode ini mencakup observasi, wawancara, dan pengumpulan fakta, serta memberikan uraian yang komprehensif. Adapun teknik analisis data yang digunakan yaitu, pengurangan data, presentasi data dan Kesimpulan.

Hasil penelitian menunjukkan bahwa: (1) Bentuk serangan yang di duga virus *ransomware* merupakan isu yang beredar tidaklah benar, melainkan adanya masalah internal yang terjadi yaitu peenambahan server data IT di Bank Syariah Indonesia. (2) Dampak serangan terkait isu virus *ransomware* yang terjadi pada Bank Syariah Indonesia Kcp Barru mulai dari penurunan nasabah, semua transaksi baik secara online maupun offline tidak bisa beroperasi dengan baik sehingga berdampak pada dana nasabah, bahkan seluruh jobdesk Bank Syariah Indonesia Kcp Barru tidak bisa melakukan pengimputan. (3) Upaya Bank Syariah Indonesia (BSI) di Kcp Barru dalam memulihkan kepercayaan nasabah setelah terjadinya serangan virus *ransomware*, dengan mengambil langkah awal untuk menjaga keamanan digital menjadi prioritas utama, melindungi data sistem nasabah maupun data rahasia bank, mengganti manajemen IT, akses ke semua perangkat komputer pegawai mulai di perketat. Bank syariah Indonesia Kcp Barru upaya yang dilakukan adalah dengan meyakinkan kembali nasabah bahwa semua dana nasabah aman dan tidak terganggu, selain itu dengan melakukan pendekatan secara kekeluargaan.

Kata kunci : Dampak virus *ransomware*, kepercayaan, nasabah, Bank Syariah Indonesia Kcp Barru, Manajemen Bank.

DAFTAR ISI

Halaman
SKRIPSI i
PERSETUJUAN KOMISI PEMBIMBING iii
PENGESAHAN KOMISI PENGUJI ..... **Error! Bookmark not defined.**
KATA PENGANTAR v
ABSTRAK ix
DAFTAR ISI x
DAFTAR GAMBAR xii
DAFTAR LAMPIRAN xiv
PEDOMAN TRANSLITERASI xv
BAB I PENDAHULUAN 1
A. Latar Belakang 1
B. Rumusan masalah 5
C. Tujuan Penelitian 5
D. Kegunaan Penelitian 5
BAB II TINJAUAN PUSTAKA 7
A. Tinjauan Penelitian Relevan 7
B. Tinjauan Teoritis 13
1. Tinjauan Tentang Konsep Dampak 13
2. Tinjauan Tentang Virus Siber 14
3. Tinjauan Tentang Sistem Informasi Manajemen Perbankan 21
4. Tinjauan Tentang Kepercayaan Nasabah 24
C. Tinjauan Konseptual 33
D. Kerangka Pikir 34
BAB III METODE PENELITIAN 36
A. Pendekatan dan Jenis Penelitian 36
B. Lokasi dan Waktu Penelitian 36
C. Fokus Penelitian 36

D. Jenis dan Sumber Data 37
E. Teknik Pengumpulan Data 37
F. Uji Keabsahan Data 38
G. Teknik Analisis Data 38
BAB IV HASIL PENELITIAN DAN PEMBAHASAN 40
A. Hasil Penelitian 40
B. Pembahasan Hasil Penelitian 52
BAB V PENUTUP 67
A. Kesimpulan 67
B. Saran 68
DAFTAR PUSTAKA 69
BIODATA PENULIS XVII

DAFTAR TABEL

No. Tabel	Judul Tabel	Halaman
2.1	Tabel Penelitian Relevan	7

DAFTAR GAMBAR

No. Gambar	Judul Gambar	Halaman
2.1	Gambar Tinjauan Teoritis	33
2.2	Bagan Kerangka Pikir	35
4.1	Grafik jumlah serangan *cyber* BSI	52
4.2	Diagram Jumlah Nasabah BSI	60

DAFTAR LAMPIRAN

No. Lampiran	Judul Lampiran	Halaman
1	Revisi Judul Skripsi	IV
2	SK Penetapan Pembimbing Skripsi	V
3	Surat Permohonan Izin Penelitian	VI
4	Surat Izin Peneltian	VII
5	Surat Keterangan Selesai Penelitian	VIII
6	Dokumentasi Wawancara	IX
7	Surat Keterangan Wawancara	XIII
8	Biodata Penulis	XVII

PEDOMAN TRANSLITERASI

A. Transliterasi

1. Konsonan

Fonem konsonan dalam bahasa Arab yang dilambangkan dengan huruf-huruf Arab, dalam sistem transliterasi ini sebagian diwakili oleh huruf, sebagian lagi oleh tanda, dan ada pula yang diwakili oleh kombinasi huruf dan tanda. Berikut adalah daftar huruf bahasa Arab beserta transliterasinya ke dalam huruf Latin:

Huruf	Nama	Huruf Latin	Nama
ا	Alif	Tidak dilambangkan	Tidak dilambangkan
ب	Ba	B	Be
ت	Ta	T	Te
ث	Tsa	Ts	te dan sa
ج	Jim	J	Je
ح	Ha	ḥ	ha (dengan titik di bawah)
خ	Kha	Kh	ka dan ha
د	Dal	D	De
ذ	Dzal	Dz	de dan zet
ر	Ra	R	Er
ز	Zai	Z	Zet
س	Sin	S	Es
ش	Syin	Sy	es dan ye
ص	Shad	ṣ	es (dengan titik di bawah)
ض	Dhad	ḍ	de (dengan titik dibawah)
ط	Ta	ṭ	te (dengan titik dibawah)
ظ	Za	ẓ	zet (dengan titik dibawah)
ع	‘ain	‘	koma terbalik ke atas
غ	Gain	G	Ge
ف	Fa	F	Ef

ق	Qaf	Q	Qi
ك	Kaf	K	Ka
ل	Lam	L	El
م	Mim	M	Em
ن	Nun	N	En
و	Wau	W	We
ه	Ha	H	Ha
ء	Hamzah	’	Apostrof
ي	Ya	Y	Ye

Hamzah (ء) di awal kata mengikuti vokalnya tanpa tanda khusus. Jika hamzah berada di tengah atau akhir kata, ditulis dengan tanda (‘).

1. Vokal

a. Vokal tunggal (monoftong) dalam bahasa Arab ditandai dengan harakat dan ditransliterasikan sebagai berikut:berikut:

Tanda	Nama	Huruf Latin	Nama
اَ	Fathah	A	A
اِ	Kasrah	I	I
اُ	Dhomma	U	U

b. Diftong dalam bahasa Arab ditandai dengan kombinasi antara harakat dan huruf, serta ditransliterasikan dengan kombinasi huruf sebagai berikut:

Tanda	Nama	Huruf Latin	Nama
ـَيْ	Fathah dan Ya	Ai	a dan i
ـَوْ	Fathah dan Wau	Au	a dan u

Contoh :

كَيْفَ : Kaifa

حَوْلَ : Haula

c. Maddah

Maddah atau vokal panjang yang ditandai dengan harakat dan huruf, serta dalam transliterasinya diwakili oleh huruf dan tanda, yaitu:

Harkat dan Huruf	Nama	Huruf dan Tanda	Nama
دَ يَا / ي	Fathah dan Alif atau ya	A	a dan garis di atas
دِ يْ	Kasrah dan Ya	I	i dan garis di atas
دُو	Kasrah dan Wau	U	u dan garis di atas

Contoh :

مات :māta

رمى : ramā

قيل : qīla

يموت : yamūtu

d. *Ta Marbutah*

Transliterasi untuk ta marbutah ada dua cara:

a. Ta marbutah yang aktif atau yang memiliki harkat fathah, kasrah, dan dammah, ditransliterasikan sebagai [t].

b. Ta marbutah yang tidak aktif atau yang memiliki harkat sukun, ditransliterasikan sebagai [h].

Jika suatu kata yang berakhir dengan ta marbutah diikuti oleh kata lain yang menggunakan kata sandang al- dan kedua kata tersebut dibaca terpisah, maka ta marbutah tersebut ditransliterasikan menjadi ha ((*h*).

Contoh :

رَوْضَةُ الجَنَّةِ : *rauḍah al-jannah atau rauḍatul jannah*

اَلْمَدِيْنَةُ الْفَاضِلَةِ : *al-madīnah al-fāḍilah atau al-madīnatul fāḍilah*

اَلْحِكْمَةُ : *al-hikmah*

e. *Syaddah* (*Tasydid*)

Syaddah atau *tasydid* yang dalam tulisan Arab diwakili oleh tanda tasydid, dalam transliterasi diwakili oleh pengulangan huruf (konsonan ganda) yang memiliki tanda *syaddah*.

Contoh:

رَبَّنَا :*Rabbanā*

نَجَّيْنَا : *Najjainā*

اَلْحَقُّ : *al-haqq*

اَلْحَجُّ : *al-hajj*

نُعْمَ : *nu‘‘ima*

عَدُوٌّ : *‘aduwwun*

Jika huruf ى memiliki tasydid di akhir kata dan diapit oleh huruf berharakat kasrah (ـِيّ), maka transliterasinya seperti huruf *maddah* (i).

Contoh:

عَرَبِيٌّ :‘Arabi (bukan ‘Arabiyy atau ‘Araby)

عَلِيٌّ : ‘Ali (bukan ‘Alyy atau ‘Aly)

f. Kata Sandang

Kata sandang dalam tulisan Arab diwakili oleh huruf "ال" (alif lam ma'arifah). Dalam panduan transliterasi ini, kata sandang ditransliterasikan sebagai "al-", baik saat diikuti oleh huruf syamsiah maupun huruf qamariah. Kata sandang ini tidak menyesuaikan dengan bunyi huruf yang mengikutinya. Kata sandang ditulis terpisah dari kata yang mengikutinya dan dihubungkan dengan tanda hubung (-).

Contoh:

اَلْشَمْسُ : *al-syamsu (bukan asy- syamsu)*
اَلزَّلْزَلَةُ : *al-zalzalah (bukan az-zalzalah)*
الفَلْسَفَةُ : *al-falsafah*
اَلْبِلَادُ : *al-bilādu*

g. Hamzah

Aturan penggunaan apostrof (') sebagai pengganti huruf hamzah diterapkan hanya ketika hamzah berada di tengah atau akhir kata. Namun, jika hamzah berada di awal kata, tidak digunakan lambang apa pun, karena dalam tulisan Arab, hamzah di awal kata diwakili oleh alif.

Contoh:

تَأْمُرُوْنَ : *ta'murūna*
النَّوعُ : *al-nau'*
شَيْءٌ : *syai'un*
أُمِرْتُ : *Umirtu*

a. Kata Arab yang lazim digunakan dalam Bahasa Indonesia

Istilah atau frasa Arab yang ditransliterasi adalah kata-kata yang belum diresmikan dalam bahasa Indonesia. Istilah atau frasa yang sudah umum dan

menjadi bagian dari kosakata bahasa Indonesia, atau yang sering muncul dalam tulisan berbahasa Indonesia, tidak lagi ditransliterasi seperti yang disebutkan di atas. Contohnya adalah Al-Qur'an dan Sunnah. Namun, jika kata-kata tersebut menjadi bagian dari teks Arab yang lengkap, maka mereka harus ditransliterasi secara penuh.

Contoh:

Fī ẓilāl al-qur'an

Al-sunnah qabl al-tadwin

Al-ibārat bi 'umum al-lafẓ lā bi khusus al-sabab

b. *Lafẓ al-Jalalah* (الله)

Kata 'Allah' yang diikuti oleh partikel seperti huruf jar dan huruf lainnya atau berfungsi sebagai mudaf ilaih dalam frasa nominal, ditransliterasikan tanpa menggunakan huruf hamzah.

Contoh:

دِيْنُ اللهِ *Dīnullah* باالله *billah*

Ta marbutah yang terletak di akhir kata dan disandarkan kepada lafẓ al-jalālah ditransliterasi menggunakan huruf [t].

Contoh:

هُمْ فِيْ رَحْمَةِ اللهِ *Hum fī rahmatillāh*

c. Huruf Kapital

Meskipun sistem tulisan Arab tidak memiliki huruf kapital, dalam proses transliterasi ini, huruf kapital digunakan sesuai dengan pedoman ejaan Bahasa Indonesia yang berlaku (EYD). Huruf kapital diterapkan untuk menulis huruf pertama dari nama-nama tertentu (seperti orang, tempat, atau bulan) dan

di awal kalimat. Ketika nama diri diikuti oleh kata sandang (al-), huruf kapital diterapkan hanya pada huruf pertama nama diri, bukan pada huruf pertama kata sandang tersebut. Namun, jika kata sandang muncul di awal kalimat, huruf A pada kata sandang tersebut ditulis dengan huruf kapital (*Al-*).

Contoh:

Wa mā Muhammadun illā rasūl

Inna awwala baitin wudi'a linnāsi lalladhī bi Bakkata mubārakan

Syahru Ramadan al-ladhī unzila fih al-Qur'an

Nasir al-Din al-Tusī

Abū Nasr al-Farabi

"Jika nama resmi seseorang mencakup istilah Ibnu (anak dari) dan Abū (bapak dari) sebagai bagian dari nama kedua terakhir, maka kedua istilah tersebut harus dicantumkan sebagai nama terakhir dalam daftar pustaka atau referensi.

Contoh:

Abū al-Walid Muhammad ibnu Rusyd, ditulis menjadi: Ibnu Rusyd, Abū al-Walīd Muhammad (bukan: Rusyd, Abū al-Walid Muhammad Ibnu) Naṣr Ḥamīd Abū Zaid, ditulis menjadi: Abū Zaid, Naṣr Ḥamīd (bukan:Zaid, Naṣr Ḥamīd Abū)

1. **Singkatan**

Beberapa akronim yang telah distandarisasi adalah:

Swt. = *subḥānahū wa ta'āla*

saw. = *ṣallallāhu 'alaihi wa sallam*

a.s. = *'alaihi al- sallām*

H = Hijriah

M = Masehi

SM = Sebelum Masehi

l. = Lahir tahun

w. = Wafat tahun

QS …/…: 4 = QS al-Baqarah/2:187 atau QS Ibrahīm/ …, ayat 4

HR = Hadis Riwayat

Berbagai akronim dalam bahasa Arab:

ص = صفحة

دم = بدون

صلعم = صلى الله عليه وسلم

ط = طبعة

دن = بدون ناشر

الخ = إلى آخرها / إلى آخره

ج = جزء

Beberapa singkatan yang digunakan secara khusus dalam teks referensi perlu dijelaskan kepanjangannya, diantaranya sebagai berikut:

Berikut adalah beberapa singkatan yang perlu dijelaskan dalam teks referensi:

ed. : Singkatan dari Editor (atau eds. jika ada lebih dari satu editor). Dalam bahasa Indonesia, "editor" mencakup baik satu maupun banyak, sehingga dapat disingkat ed. tanpa s.

et al. : Berarti "dan lain-lain" atau "dan kawan-kawan" (dari et alia), ditulis miring. Sebagai alternatif, dapat digunakan dkk. yang ditulis dengan huruf biasa.

Cet. : Merupakan singkatan dari cetakan, menggambarkan frekuensi cetakan buku atau literatur serupa.

Terj. : Singkatan untuk terjemahan (oleh), digunakan dalam karya terjemahan tanpa mencantumkan nama penerjemah.

Vol. : Singkatan dari volume, menunjukkan jumlah jilid dalam buku atau ensiklopedi berbahasa Inggris. Dalam konteks buku berbahasa Arab, istilah yang digunakan adalah juz.

No. : Singkatan dari nomor, digunakan untuk menunjukkan nomor dalam publikasi ilmiah berkala seperti jurnal atau majalah.sebagainya.

BAB I

PENDAHULUAN

A. Latar Belakang

Dengan kemajuan teknologi internet, sering muncul berbagai masalah akibat penyalahgunaan. Di sisi lain, penggunaan internet yang hampir tidak teratur dapat memicu berbagai kejahatan di dunia maya, yang belakangan ini dikenal sebagai "Cyber Crime" [1] Di Indonesia, terdapat berbagai kejahatan seperti pencurian informasi kartu kredit, peretasan situs web, penyadapan data pribadi seperti email, serta manipulasi data melalui pengaturan perintah yang tidak diinginkan dalam perangkat lunak. [2] Kejahatan siber juga merupakan masalah di Indonesia, dan sebenarnya telah muncul sejak kedatangan internet di negara ini. Berdasarkan informasi dari perusahaan keamanan siber Surfshark, pada kuartal kedua tahun 2022, terdapat 1,04 juta akun yang mengalami kebocoran data di Indonesia.

Pada kuartal kedua 2022, kasus kebocoran data di Indonesia meningkat tajam sebesar 143% dibandingkan kuartal pertama 2022. [3] Berbagai entitas, mulai dari perusahaan swasta hingga lembaga pemerintah, tidak terhindar dari kejahatan ini. Dampaknya dapat berkisar dari perubahan tampilan dan suasana situs web hingga pengungkapan data pribadi warga Indonesia. Selain itu, peretas juga bisa mencuri atau membagikan informasi yang tersimpan di komputer. Untuk mengakses kembali data yang terkunci, korban seringkali diwajibkan membayar tebusan kepada penyerang, biasanya dalam bentuk mata uang kripto. Salah satu contoh kasus serangan *ransomware* yang pernah terjadi di Indonesia yang cukup menggegerkan public yaitu serangan pada Bank Indonesia (BI). Pada 21 Januari 2022, serangan ini

[1] "cyber crime" merupakan sebagai suatu kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara illegal.

[2] Yuni Fitriani and Roida Pakpahan, "Analisa Penyalahgunaan Media Sosial Untuk Penyebaran Cybercrime Di Dunia Maya Atau Cyberspace," *Cakrawala : Jurnal Humaniora* 20, no. 1 (2020): 2579–3314.

[3] Achmad Farid, "14 Kasus Cyber Crime Di Indonesia Yang Menggemparkan Warganet," Exabytes, 2022

dikatakan menyerang computer personal BI di kantor Bengkulu. Setelah ditelusuri, ada sekitar 16 komputer yang terdampak.[4] Maraknya kejahatan siber di dalam perbankan mungkin meningkat, seperti yang baru-baru ini terjadi pada BSI. Kejadian penyerangan virus terhadap Bank Syariah Indonesia yang di duga virus *malware* itu terjadi pada tanggal 08 Mei 2023 yang mengakibatkan nasabah tidak bisa bertransaksi. Serangan yang diduga berasal dari virus *ransomware* terhadap BSI terungkap setelah pelanggan bank mengeluhkan di media sosial mengenai ketidakmampuan mereka mengakses aplikasi mobile banking BSI. Kelompok yang melakukan serangan ini, yang dikenal sebagai LockBit 3.0, memanfaatkan metode phishing dan lampiran berbahaya.[5] untuk "untuk menginfeksi sistem perbankan dengan *Ransomware*.[6]

Penjelasan mengenai pelaku kerusakan dapat ditemukan dalam Qur'an surah Al-Baqarah 2:205 sebagai berikut :

وَاِذَا تَوَلّٰى سَعٰى فِى الْاَرْضِ لِيُفْسِدَ فِيْهَا وَيُهْلِكَ الْحَرْثَ وَالنَّسْلَۗ وَاللّٰهُ لَا يُحِبُّ الْفَسَادَ

Terjemahnya :

> Apabila berpaling (dari engkau atau berkuasa), dia berusaha untuk berbuat kerusakan di bumi serta merusak tanam-tanaman dan ternak. Allah tidak menyukai kerusakan.[7]

Maksudnya : ayat diatas menjelaskan pelaku yang membuat kerusakan di muka bumi yang merusak tanaman dan ternak. artinya, bagaimana para pelaku serangan virus *ransomware* yang diduga melakukan penyerangan sistem

[4] Zulfikar Hardiansyah, "Kasus Serangan *Ransomware* Di Indonesia, BI Pernah Jadi Sasaran," accessed July 27, 2024

[5] *Malicious attachments* merupakan lampiran berbahaya adalah file yang dikirim dengan email yang dirancang untuk membahayakan atau merusak sistem komputer penerima atau mengeksfiltrasi informasi sensitif

[6] Gratiyo Wahyu Wahidin, Syaifuddin Syaifuddin, and Zamah Sari, "Analisis *Ransomware* Wannacry Menggunakan Aplikasi Cuckoo Sandbox," *Jurnal Repositor* 4, no. 1 (2022): 83–94,

[7] Kementerian Agama RI, "Al-Qur'an Dam Terjemahannya, Q.S. Al-Baqarah, 205," 2019.

keamanan Bank Syariah Indonesia (BSI) sehingga menyebabkan kerugian yang besar.

Pada kasus ini, serangan telah menyebabkan kerugian data sebesar 1,5 TB, termasuk informasi sensitif pelanggan.[8] Akibatnya serangan tersebut berdampak pada transaksi *Automatic Teller Machine* (ATM), error pada applikasi BSI *mobile banking* sehingga membuat para nasabah yang ingin melakukan transaksi secara online terhambat. Menurut ahli keamanan siber dan forensik digital, Alfnos Tanujaya, ransomware berupaya sekuat mungkin untuk mengenkripsi data penting, cadangan, dan sistem dengan tujuan mengganggu operasi perusahaan.[9]

Internet banking atau perbankan internet atau perbankan *mobile* adalah layanan yang memungkinkan nasabah melakukan transaksi keuangan melalui internet. Layanan ini memanfaatkan teknologi digital untuk melakukan berbagai transaksi dan mengakses informasi lainnya melalui situs web resmi bank. Nasabah dapat berinteraksi dengan bank tanpa perlu mengunjungi kantor fisik, cukup menggunakan perangkat seperti komputer, laptop, tablet, atau *smartphone* yang terhubung ke internet. Untuk menggunakan layanan ini, nasabah perlu memiliki *user* ID, *password*, token, atau *One Time Password* (OTP), yang bisa didapatkan dengan mendaftar di bank. Saat mengakses layanan perbankan internet, penting bagi nasabah untuk memastikan bahwa mereka mengunjungi situs web resmi bank, lalu memasukkan *user* ID dan *password* pada halaman *login*. Untuk transaksi finansial, nasabah harus memasukkan OTP yang diterima dari token. Setelah menyelesaikan transaksi, penting untuk keluar dari akun *internet banking*. Bank akan mengirimkan notifikasi melalui email sebagai konfirmasi bahwa transaksi telah berhasil.[10]

---

[8] Rajani S. Sajjan and Vijay R. Ghorpade, "*Ransomware* Attacks: Radical Menace for Cloud Computing," *Proceedings of the 2017 International Conference on Wireless Communications, Signal Processing and Networking, WiSPNET 2017* 2018-January, no. March 2017 (2017): 1640–46,

[9] Edward Ricardo, "BSI Diserang *Ransomware*, Nasib Uang Nasabah Gimana?," Redaksi, CNBC Indonesia, 2023

[10] Shinhan Bank, "Pengertian Internet Banking," Shinhan Bank, 2017.

Internet banking adalah penggunaan internet oleh bank untuk mempromosikan dan melaksanakan transaksi secara daring, baik untuk produk konvensional maupun yang inovatif. Agar layanan ini memberikan manfaat finansial, bank perlu menjadikannya bagian dari strategi multichannel yang memungkinkan nasabah mengakses layanan kapan saja dan di mana saja. Untuk mendukung strategi tersebut, bank harus menyediakan layanan internet banking yang real-time dan memberikan tampilan menyeluruh terhadap informasi nasabah. Dengan pendekatan ini, bank dapat merespons setiap interaksi atau transaksi dengan cepat dan meningkatkan pengalaman nasabah. Namun, meskipun memberikan kemudahan, layanan internet banking juga menghadirkan sejumlah risiko yang perlu diperhatikan sebagaimana dalam menjaga kualitas nasabah maupun kepercayaan nasabah bank yang dimiliki.[11]

Kepercayaan nasabah sejatinya sangat di tentukan oleh kinerja bank termasuk pengelolaan keuangan yang *prudent.* Namun, betapapun sebuah bank telah memiliki kinerja dan pengelolaan keuangan yang baik dari prespektif *marketing* bank harus[12] mampu menunjukkan kualitas pelayanan yang prima sehingga nasabah merasa nyaman dan menumbuhkan kepercayaan. Selain itu, dapat dikatakan bahwa kualitas pelayanan yang disuguhkan merupakan daya tarik yang cukup menggoda asyarakat dalam menggunakan jasa perbankan. Sedangkan untuk meningkatkan loyalitas nasabah sangat didukung oleh adanya kepercayaan nasabah yang tinggi dan terus menerus.

Berdasarkan penelitian sebelumnya, telah dilakukan beberapa studi, namun ada perbedaan antara penelitian tersebut dan penelitian yang akan dilaksanakan. Dimana studi ini membahas bagaimana dampak yang diberikan serangan virus *ransomware* dan befokus pada kepercayaan nasabah BSI dalam menyimpan dana di

[11] Nuramaliah Fakhriani Usman, "Prefrensi Nasabah Terhadap Penggunaan Layanan Internet Bangking Di Bank Mandiri Parepare," *Skripsi*, 2020. Hal. 2

[12] Yuli Andesra, "Peran Kualitas Pelayanan Dalam Mebangun Kepercayaan Dan Loyalitas Nasabah Bank Syariah Mandiri Cabang Simpang Empat," *Jurnal Apresiasi Ekonomi* 4, no. 2 (2019): 138–50

salah satu kantor cabang, sedangkan beberapa penelitian terdahulu hanya membahas pada serangan *ransomware* yang menyerang system BSI dan belum berfokus pada kepercayaan dan kepuasaan nasabah. Maka penulis ingin melakukan penelitian untuk mengetahui apakah serangan virus *ransomware* memiliki dampak terhadap kepercayaan nasabah dalam penyimpanan dana di BSI KCP Barru.

B. Rumusan masalah

1. Bagaimana bentuk serangan yang diduga virus *ransomware* terhadap Bank Syariah Indonesia (BSI) Kcp Barru?
2. Bagaimana dampak serangan virus *ransomware* terhadap kepercayaan nasabah di terhadap Bank Syariah Indonesia (BSI) Kcp Barru?
3. Bagaimana upaya terhadap Bank Syariah Indonesia (BSI) Kcp Barru dalam memulihkan tingkat kepercayaan nasabah setelah terjadinya serangan virus *ransomware*?

C. Tujuan Penelitian

Penulis memiliki tujuan dan manfaat yang ingin dicapai melalui penelitian ini, sebagai berikut:

1. Untuk mengetahui bentuk serangan yang diduga Virus *Ransomware* Terhadap Bank Syariah Indonesia (BSI) Kcp Barru.
2. Untuk mengetahui dampak serangan virus terhadap tingkat kepercayaan nasabah di Bank Syariah Indonesia (BSI) Kcp Barru.
3. Untuk mengetahui upaya Bank Syariah Indonesia (BSI) Kcp Barru dalam memulihkan tingkat kepercayaan nasabah setelah terjadinya serangan virus *ransomware*.

D. Kegunaan Penelitian

1. Kegunaan Teoritis

a.Sebagai sumber referensi atau literatur untuk memperkaya informasi dalam penelitian yang berkaitan dengan isu serupa.

b. Untuk mendukung perkembangan ilmu pengetahuan, khususnya dalam sektor perbankan syariah, mengenai dampak serangan virus *ransomware* yang berdampak pada kepercayaan nasabah.

2. Kegunaan Praktis

a. Untuk Peneliti

Bermanfaat dalam memperluas pemahaman dan pengetahuan mengenai dampak serangan virus *ransomware* terhadap kepercayaan nasabah.

b. Untuk Bank

Dapat digunakan sebagai sumber referensi untuk mempelajari dampak serangan *ransomware* terhadap kepercayaan nasabah dalam sektor perbankan.

c. Untuk Perpustakaan IAIN Parepare

Berfungsi sebagai acuan bagi peneliti berikutnya dalam membahas isu terkait serangan *ransomware*.

BAB II

TINJAUAN PUSTAKA

A. Tinjauan Penelitian Relevan

Tinjauan hasil penelitian ini membandingkan dengan studi-studi sebelumnya, yang bertujuan untuk memastikan bahwa penelitian ini asli dan bukan plagiarisme. Beberapa tulisan yang dihasilkan dari penelitian tersebut memiliki hubungan langsung maupun tidak langsung dengan topik proposal ini, khususnya mengenai Dampak Serangan Virus Ransomware terhadap Kepercayaan Nasabah dalam Penyimpanan Dana di BSI KCP Barru.

Sebagai pertimbangan dalam penelitian ini, akan disertakan beberapa hasil penelitian sebelumnya yang relevan, baik dari segi judul, objek, maupun subjek yang berhubungan dengan studi yang dilakukan oleh peneliti.

Tabel 2.1
Penelitian Relevan

No	Nama	Judul	Hasil	Perbedaan dan Persamaan
1	Kaira Milani Fitria (2023)	Analisis Serangan *Malware* Dalam Perbankan Dan Perencanaan Solusi Keamanan.	Hasil eksplorasi menunjukkan beragam solusi keamanan yang dikembangkan untuk mengatasi ancaman terhadap mobile banking. Penelitian ini dengan teliti menganalisis keterbatasan yang ada dan mengeksplorasi	**Perbedaan :** Terletak pada perencanaan solusi keamanan yang di teliti dan metode pada penelitian ini berbeda. **Persamaan :** Letak persamaannya membahas pada serangan virus siber pada bank.

			kemungkinan perbaikan sistem. Meskipun solusi keamanan tersebut menawarkan landasan yang kuat dalam melawan ancaman *malware* di mobile banking, penting untuk disadari bahwa ancaman baru akan terus muncul dan berkembang.	
2	Rendi Panca Wijanarko, *et al*. (2023)	Analisis Dan Simulasi Serangan Ransomware Terhadap Database Bank Syariah Indonesia	Berdasarkan penelitian ini, disarankan kepada pembaca untuk secara rutin melakukan pencadangan data dan memastikan perangkat cadangan tidak berada di dekat perangkat operasional utama. Hal ini akan memudahkan proses pemulihan data setelah terjadinya serangan. Dengan langkah-langkah tersebut, diharapkan risiko serangan	**Perbedaan :** Terletak pada Analisis dan simulasi terhadap database dan metode pada penelitian ini yang digunakan berbeda. **Persamaan :** Membahas serangan ransomware dan objek penelitian pada Bank Syariah Indonesia (BSI).

			ransomware dapat diminimalkan dan perlindungan terhadap basis data dapat dilakukan secara efektif.	
3	Mutmainnah (2021)	Tingkat Kepercayaan Nasabah Bmi Cabang Parepare Dalam Menggunakan Internet Bangking Dan Transaksi Langsung.	Ada hasil yang di tunjukkan melalui 2 data : 1. data primer menunjukkan dari hasil wawancara membuktikan bahwa nasabah hamper semua menggunakan transaksi secara langsung 2. Data sekunder menunjukkan bahwa dalam satu bulan penggunaan internet banking mencapai 28%, sementara transaksi secara langsung tercatat sebesar 78%. "Ini mengindikasikan bahwa	**Perbedaan :** Terletak pada subjek penelitian yaitu, Dalam Menggunakan Internet Bangking Dan Transaksi Langsung. **Persamaan :** Dilihat dari tingkat kepercayaan nasabah dan metode yang digunakan.

			kepercayaan nasabah dalam melakukan transaksi langsung lebih besar dibandingkan dengan menggunakan internet banking.	
4	Sumarni (2021)	Pengaruh Nisbah Bagi Hasil Terhadap Kepercayaan Nasabah Di Bni Syariah Kcp Wonomulyo.	Nisbah bagi hasil memiliki pengaruh positif dan signifikan terhadap tingkat kepercayaan nasabah BNI Syariah KCP Wonomulyo.	**Perbedaan :** Subjek penelitian Pengaruh Kualitas Layanan Terhadap Kepuasaan dan metode penelitian yang digunakan. **Persamaan :** Kepercayaan dan nasabah.
5	Anita Rahayu (2021)	Strategi Customer Service Dalam Manajemen Complain Automatic Teller Machine (Atm) Pada Btn Syariah Parepare.	Strategi layanan pelanggan dalam menangani keluhan nasabah diterapkan sesuai dengan standar Bank BTN Syariah Parepare. Implementasi strategi ini berdampak signifikan pada kepuasan dan loyalitas nasabah, serta menjaga citra bank tetap positif di mata nasabah dan masyarakat.	**Perbedaan :** Terletak pada subjek penelitian dapat dilihat dari judul penelitian. **Persamaan :** Dapat dikatakan bahwa permasalahan yang diangkat dari penelitian ini hampir sama yang berasal dari komplain nasabah terhadap manajemen pihak bank, yang bepengaruh terhadap hasil

				penelitian, yaitu tingkat kepuasan nasabah selain itu, metode kualitatif yang digunakan.

Berdasarkan Tabel 2.1, terlihat bahwa penelitian-penelitian tersebut relevan dengan studi yang sedang berlangsung. Salah satunya adalah penelitian Kaira Milani pada tahun 2023 yang berjudul "Analisis Serangan *Malware* Dalam Perbankan Dan Perencanaan Solusi Keamanan." Penelitian ini bertujuan untuk menganalisis secara menyeluruh berbagai jenis serangan *malware* dalam sektor perbankan serta merancang solusi keamanan yang dapat menekan risiko tersebut. Metode yang digunakan pada pelitian ini melibatkan tinjauan komprehensif. Perbedaan pada subjek penelitian yaitu, Terletak pada perencanaan solusi keamanan yang di teliti dan metode yang digunakan pada penelitian ini berbeda sedangakan persamaannya yaitu, membahas pada serangan virus siber pada bank.[13]

Penelitian kedua dari Rendi Panca Wijanarko, *et al*. tahun 2023 dengan judul "Analisis Dan Simulasi Serangan Ransomware Terhadap Database Bank Syariah Indonesia" Studi ini bertujuan untuk mengidentifikasi potensi kerentanan dan efek dari serangan ransomware pada infrastruktur database suatu organisasi. Metode yang diterapkan dalam penelitian ini meliputi tinjauan pustaka yang relevan, pengamatan terhadap kasus serangan ransomware, serta simulasi serangan sistem. Perbedaan pada subjek penelitian yaitu, terletak pada Analisis dan simulasi terhadap database dan metode pada penelitian ini yang digunakan berbeda sedangkan persamaannya yaitu,

[13] Kaira Milani Fitria, "Analisis Serangan *Malware* Dalam Perbankan Dan Perencanaan Solusi Keamanan," *Institut Informatika Dan Bisnis Darmajaya* 11, no. 3 (2023)

membahas serangan ransomware dan objek penelitian pada Bank Syariah Indonesia (BSI).[14]

Penelitian ketiga dari Mutmainnah tahun 2021 dengan judul "Tingkat Kepercayaan Nasabah Bmi Cabang Parepare Dalam Menggunakan Internet Bangking Dan Transaksi Langsung" penelitian ini bertujuan untuk mengukur tingkat kepercayaan nasabah terhadap penggunaan internet banking dan transaksi langsung. Penelitian ini menggunakan metode lapangan dengan pendekatan deskriptif dan kualitatif. Data dikumpulkan melalui wawancara, yang kemudian dianalisis untuk memberikan gambaran tentang subjek penelitian terkait internet banking dan transaksi langsung. Namun, ada juga persamaannya yaitu tingkat kepercayaan nasabah.[15]

Penelitian keempat dari Sumarni tahun 2021 dengan judul "Pengaruh Nisbah Bagi Hasil Terhadap Kepercayaan Nasabah Di Bni Syariah Kcp Wonomulyo" Studi ini bertujuan untuk mengeksplorasi apakah terdapat pengaruh antara nisbah bagi hasil dan kepercayaan nasabah, dengan nisbah bagi hasil sebagai variabel independen dan kepercayaan nasabah sebagai variabel dependen. Penelitian ini menggunakan pendekatan deskriptif kuantitatif, dan data diperoleh melalui kuesioner dan dokumentasi. Penelitian ini juga membedakan subjek yang diteliti yakni, Pengaruh Nisbah Bagi Hasil dan metode penelitian yang digunakan. Namun terdapat persamaan yaitu dampak yang di berikan terhadap kepercayaan nasabah.[16]

Penelitian kelima dari Anita Rahayu tahun 2021 degan judul "Strategi *Customer Service* Dalam Manajemen komplain *Automatic Teller Machine* (Atm) Pada Btn Syariah Parepare" tujuannya untuk mengidentifikasi strategi layanan

[14] Rendi Panca Wijanarko et al., "Analisis Dan Simulasi Serangan *Ransomware* Terhadap Database Bank Syariah Indonesia," *Universitas Pembanguan Nasioanal (UPN) Veteran Jakarta* 3, no. 1 (2023): 106–15

[15] Mutmainnah, "Tingkat Kepercayaan Nasabah BMI Cabang Parepare Dalam Menggunakan Internet Bangking Dan Transaksi Langsung," *Institut Agama Islam Negeri*, 2021.

[16] Sumarni, "Pengaruh Nisbah Bagi Hasil Terhadap Kepercayaan Nasabah DI BNI Syariah KCP Wonomulyo," *Institut Agama Islam Negeri*, 2021.

pelanggan dalam menangani keluhan nasabah mengenai masalah pada *Automatic Teller Machine* (ATM), serta untuk memahami dampak dari pengelolaan keluhan yang dilakukan oleh layanan pelanggan terhadap nasabah. Metode yang diterapkan dalam penelitian ini adalah pendekatan kualitatif, dengan pengumpulan data primer melalui observasi, wawancara, dan dokumentasi. Penelitian ini memiliki perbedaan pada subjek penelitian dapat dilihat dari judul penelitian dan persamaannya dari penelitian ini masalah yang diangkat hampir sama yang berasal dari komplain nasabah terhadap manajemen pihak bank, yang bepengaruh terhadap hasil penelitian, yaitu tingkat kepuasan nasabah.[17]

B. Tinjauan Teoritis

1. Tinjauan Tentang Konsep Dampak

"Dampak, menurut Kamus Lengkap Bahasa Indonesia, diartikan sebagai pengaruh dari suatu hal yang menghasilkan konsekuensi; benturan; yang cukup signifikan sehingga dapat menyebabkan perubahan.[18] Secara etimologis, istilah "dampak" merujuk pada pelanggaran, tubrukan, atau benturan. Awalnya, istilah ini digunakan sebagai padanan untuk kata "*impact*" dalam Bahasa Inggris. Dalam konteks Bahasa Inggris, "*impact*" berarti tabrakan atau benturan.[19]

Menurut Kamus Besar Bahasa Indonesia, dampak merujuk pada benturan atau pengaruh yang signifikan yang menghasilkan konsekuensi, baik itu berupa dampak negatif maupun positif. Akibat, menurut definisi dalam Kamus Besar Bahasa Indonesia, mengacu pada hasil atau konsekuensi dari suatu peristiwa, keputusan, atau keadaan yang terjadi sebelumnya.[20] Dampak merupakan hasil dari suatu tindakan, yang bisa bersifat positif atau negatif, serta menciptakan

---

[17] Anita Rahayu, "Strategi Customer Service Dalam Manajemen Komplain Automatic Teller Machine (ATM) Pada Bank BTN Syariah Parepare," *Institut Agama Islam Negeri*, 2021.

[18] Suharno and Retnoningsih, *Kamus Besar Bahasa Indonesia* (Semarang: Widya Karya, 2003). h. 243

[19] Soerjono Soekanto, *Sosiologi Suatu Pengantar*, Revisi (Jakarta: Rajawali Pers, 2017). h. 380

[20] Lily Nur Indah Sari, "Dampak Pembiayaan BNI Syariah Kcp Wonomulyo Terhadap Peningkatan UMKM," *Institut Agama Islam Negeri Parepare* 10, no. 2 (2021): 10,

pengaruh yang kuat dengan konsekuensi baik atau buruk. Adapun dampak secara umum merujuk pada segala sesuatu yang muncul sebagai akibat dari adanya suatu hal. Dampak ini dapat bersifat signifikan, dengan konsekuensi yang dirasakan sebelum dan setelah terjadinya hal tersebut.[21]

Dari berbagai pendapat yang telah disampaikan, dapat disimpulkan bahwa dampak merujuk pada perubahan yang timbul akibat aktivitas atau tindakan yang dilakukan sebelumnya, sebagai konsekuensi dari pelaksanaan suatu kebijakan, yang dapat membawa perubahan baik yang positif maupun negatif.[22]

2. Tinjauan Tentang Virus Siber

a. Pengertian Virus Siber

Virus komputer adalah jenis perangkat lunak yang sering kali tersembunyi dalam program lain yang terlihat aman. Virus ini dapat memperbanyak dirinya dan menyisipkan salinan ke dalam program atau file lain, biasanya dengan tujuan melakukan tindakan merusak, seperti menghapus data. Salah satu contohnya adalah infeksi PE, sebuah metode yang umum digunakan untuk menyebarkan *malware*, di mana data tambahan atau kode yang dapat dieksekusi disisipkan ke dalam file PE.[23]

Menurut Kamus Besar Bahasa Indonesia (KBBI), istilah "siber" merujuk pada sistem komputer dan informasi, serta hal-hal yang terkait dengan internet. Dalam buku "*Cyber Security Policy Guidebook"* mengartikan keamanan siber dari sudut pandang kebijakan publik sebagai perlindungan yang dirancang untuk menjaga segala sesuatu yang ada di dunia maya. Secara umum, keamanan siber mencakup penggunaan orang, proses,

[21] Sinta Hariyati, "Persepsi Masyarakat Terhadap Pembangunan Jembatan Mahkota Ii Di Kota Samarinda," *Journal Ilmu Pemerintahan* 3, no. 2 (2008): 585–96.

[22] Lily Nur Indah Sari, "Dampak Pembiayaan BNI Syariah Kcp Wonomulyo Terhadap Peningkatan UMKM." *Institut Agama Islam Negeri Parepare* 10, no. 2 (2021): h. 12

[23] "*Malware*," Wikipedia bahasa Indonesia, ensiklopedia bebas, 2023

dan teknologi untuk mencegah, mendeteksi, dan memulihkan kerusakan yang dapat mengancam kerahasiaan, integritas, dan ketersediaan informasi di ranah siber.

Penjelasan Bayuk di atas berasal dari terjemahan bukunya. "*Cyber security is Security modified with an adjective referring to the cyberspace properties of the thing to be secured. In general, cyber security refers to methods of using people, process, and technology to prevent, detect, and recover from damage to confidentiality, integrity, and availability of information in cyberspace*".

Menurut Stevens dalam bukunya "*Cyber Security and the Politics of Time*", keamanan siber dilihat dari sudut pandang politik sebagai respons terhadap risiko dan ancaman kontemporer yang dihadapi oleh infrastruktur teknologi informasi global, yang sering kali diidentifikasi dengan istilah "internet". Secara umum, ini mencakup semua individu atau entitas yang terlibat dalam komunikasi digital atau elektronik.

Dapat disimpulkan bahwa keamanan siber merupakan suatu pendekatan yang melibatkan individu, prosedur, dan teknologi untuk mengidentifikasi, mendeteksi, mencegah (melindungi), menanggapi, dan memulihkan dari kerusakan pada kerahasiaan, integritas, dan ketersediaan informasi digital.[24]

Siber dalam Bahasa Indonesia diambil dari istilah Inggris "*cyber*". Secara umum, siber merujuk pada segala sesuatu yang berkaitan dengan sistem komputer dan informasi. Seiring waktu, istilah ini juga mencakup aspek yang berhubungan dengan internet. Siber meliputi berbagai bidang dalam ilmu komputer, seperti penyimpanan, perlindungan, akses, pemprosesan, transmisi, dan penghubungan data.[25]

---

[24] Baderi Imam Muchdi, "'Definisi Keamanan Siber (*Cyber Security*),'" Kompasiana.com, 2020

[25] Kanal Informasi, "Pengertian Siber (*Cyber*)," lentera kecil grup, 2023

b. Macam-Macam Virus

Konteks serangan siber, ada beberapa jenis yang patut mendapatkan perhatian khusus. Setiap serangan ini biasanya memiliki metode penanganan dan sistem keamanan yang unik.

1. Malware

Fenomena yang paling umum dijumpai adalah *malware*, yang merujuk pada perangkat lunak berbahaya. Ini merupakan senjata utama bagi penyerang siber, digunakan oleh para penjahat atau peretas untuk mengganggu atau merusak sistem pengguna yang sah.

Malware, yang merupakan singkatan dari perangkat lunak berbahaya, merujuk pada program yang secara khusus dirancang untuk merusak komputer, server, klien, atau jaringan. Berbeda dengan perangkat lunak yang rusak karena kesalahan, *malware* termasuk berbagai jenis, seperti virus, *worm*, trojan, *ransomware*, *spyware*, *adware*, dan *scareware*. Selain itu, program dapat dikategorikan sebagai *malware* jika secara diam-diam bertindak melawan kepentingan pengguna. Contohnya, pada suatu waktu, disk musik kompak Sony secara tersembunyi menginstal *rootkit* di komputer pembeli untuk mencegah penyalinan ilegal, tetapi juga melaporkan kebiasaan mendengarkan pengguna, yang menciptakan kerentanan keamanan tambahan.

Jenis perangkat lunak antivirus, *firewall*, dan strategi lainnya digunakan untuk melindungi sistem dari ancaman *malware*, mendeteksi keberadaan *malware*, dan memulihkan dari serangan berbahaya. *Malware* dapat menyerang file pribadi dan memperbanyak dirinya, yang dapat merusak hard disk dan perangkat lunak, mencuri data, serta mengganggu sistem informasi pada komputer yang disasar. *Malware* dapat berupa program atau kode yang menyamar sebagai pengguna dan

menjalankan sistem tanpa izin. Perangkat lunak ini dapat merusak dengan memanipulasi program atau menghentikannya. Beberapa *malware* yang berbahaya bahkan mampu menonaktifkan perangkat lunak antivirus yang terpasang di sistem.[26]

2. Phishing

Phishing merupakan bentuk kejahatan siber di mana pelaku menghubungi korban melalui email, telepon, atau pesan teks, menyamar sebagai institusi resmi, untuk menipu individu agar menyerahkan informasi sensitif. Data yang dicuri, seperti identitas pribadi, rincian kartu kredit, dan kata sandi, kemudian dapat digunakan untuk mengakses akun penting, yang berpotensi mengakibatkan pencurian identitas dan kerugian finansial.

3. Denial of Service (DDoS)

DDoS, atau serangan penolakan layanan terdistribusi, merupakan ancaman siber di mana pelaku kejahatan berusaha mengganggu server, layanan, atau lalu lintas normal dari jaringan tertentu. Mereka melakukannya dengan membanjiri target atau infrastruktur sekitarnya dengan lalu lintas internet yang berasal dari berbagai alamat IP. Akibatnya, sistem dapat menjadi tidak dapat diakses, server mengalami overload, atau bahkan terpaksa offline sementara, yang mengganggu fungsi penting organisasi.

c. Pengertian Virus *Ransomware*

Ransomware merupakan jenis *malware* yang dirancang oleh *hacker*. Perangkat lunak ini mengenkripsi file dan data pengguna pada perangkat, sehingga menjadi tidak dapat diakses atau dihapus. Para pelaku kejahatan kemudian meminta uang tebusan untuk proses dekripsi.

[26] Mark Russinovich, "Sony, Rootkits and Digital Rights Management Gone Too Far," Mark's Blog, 2019

Mengembalikan file yang terinfeksi *ransomware* sangat sulit dan hampir tidak mungkin. Pilihan yang ada adalah menginstal ulang hard disk atau tidak menggunakannya sama sekali. Selain itu, biaya untuk mendekripsi file yang terkena *ransomware* juga cukup tinggi.

Ransomware merupakan salah satu tipe *malware* yang menggunakan enkripsi untuk mengubah data menjadi format yang tidak bisa dibaca oleh perangkat. Hal ini mengakibatkan korban tidak dapat mengakses perangkat mereka hingga data tersebut didekripsi, yaitu dikembalikan ke bentuk aslinya. Untuk mendekripsi data di perangkat yang terinfeksi, pengguna perlu mendapatkan kode dekripsi yang biasanya ditawarkan oleh peretas setelah membayar tebusan. Jika dalam waktu tertentu tidak berhasil mendekripsi, maka data di perangkat tersebut bisa hilang.

Jenis *malware* yang ada, *ransomware* tergolong yang paling berbahaya. Berbeda dengan *malware* lain, *ransomware* dapat merusak sistem perangkat hingga tidak dapat berfungsi. Selain itu, *ransomware* juga memiliki kemampuan untuk menyebar dan menginfeksi perangkat lain di sekitarnya, sehingga penanganannya harus segera dilakukan untuk mencegah dampak yang lebih parah.[27]

d. Bentuk-bentuk Virus *Ransomware*

Ransomware hadir dalam berbagai bentuk dan jenis, mencapai ratusan atau bahkan ribuan, masing-masing dengan karakteristik yang berbeda. Secara umum, ada dua kategori utama *ransomware*:

[27] Mike Napizahni, "Apa Itu *Ransomware*? Pengertian, Jenis, Dan Cara Mengatasinya," PT Dewaweb, 2022.

1. Locker *Ransomware* (Non-Enkripsi)

Locker ransomware menghalangi akses pengguna dengan mengunci layar (*lock-screen*) perangkat. Setelah layar terkunci, pelaku akan meminta tebusan agar akses dapat dipulihkan.

2. *Ransomware Cryptolocker* (Enkripsi)

Ransomware jenis ini, yang sering dipakai oleh pelaku kejahatan siber, mengenkripsi file digital di komputer korban. Pelaku kemudian meminta uang tebusan untuk memberikan kunci dekripsi.[28]

e. Ciri-ciri Virus *Ransomware*

Berikut adalah beberapa tanda bahwa perangkat Anda mungkin telah terinfeksi oleh virus *ransomware*:

1. Semua format file, seperti video, foto, dan dokumen lainnya, berubah menjadi format tertentu dan tidak bisa diakses.
2. Data atau file di perangkat lain bisa terinfeksi setelah menggunakan flashdisk atau media penyimpanan lain yang sebelumnya dipakai di perangkat Anda.
3. Anda akan menerima pesan dari *hacker*, biasanya berupa file *teks*, yang berisi ancaman dan permintaan tebusan.
4. Dalam pesan tersebut terdapat informasi mengenai drive C: *System*, yang mencakup *Personal ID* dengan kode unik sebagai cara untuk membuka akses ke file yang terkunci.[29]

f. Faktor-faktor yang Mempengaruhi Terjadinya Virus *Ransomware*

Berikut adalah beberapa faktor penyebab *ransomware*:

[28] Nur Syamsi Tajriyani, "Pertanggungjawaban Pidana Tindak Pidana Pemerasan Dengan Modus Operandi Penyebaran *Ransomware* Cryptolocker," *Jurist-Diction* 4, no. 2 (2021): 685

[29] Ahmad Nur Ubaidah, "Tipe Virus *Ransomware* Dan Solusi Terbaik Mengatasinya," Logique, 2021

1. *Phishing*

Ransomware sering menyebar melalui email phishing, di mana penyerang berusaha memperoleh informasi sensitif dengan cara menipu korban agar memasukkan data pribadi atau mengklik tautan berbahaya.

2. Kelemahan Keamanan

Serangan dapat memanfaatkan celah dalam sistem keamanan. Jika sistem tidak mendapatkan pembaruan atau *patch* yang diperlukan, penyerang dapat mengambil alih dan mengenkripsi data.

3. Perangkat Lunak Palsu

Ransomware juga dapat ditransmisikan melalui perangkat lunak palsu yang tampak seperti aplikasi sah. Setelah diunduh, perangkat ini bisa menginstal *ransomware* di sistem korban.

4. Jaringan yang Tidak Aman

Penyebaran juga bisa terjadi di jaringan yang kurang terlindungi. Begitu *ransomware* masuk, ia dapat menyebar dengan cepat ke sistem lain dalam jaringan tersebut.

5. Pembayaran *Ransomware*

Beberapa korban memilih membayar tebusan untuk mendapatkan kembali akses ke data mereka. Tindakan ini dapat memicu penyerang untuk terus melancarkan serangan dan mengembangkan metode yang lebih rumit.[30]

[30] Aulia Reta Faulina, "Apa Itu *Ransomware*, Jenis, Penyebab, Dan Cara Mencegahnya," Sekawan Media, 2023

3. Tinjauan Tentang Sistem Informasi Manajemen Perbankan

Sistem informasi manajemen saat ini tidak hanya berfungsi untuk memenuhi kebutuhan manajemen di berbagai level dan departemen, tetapi juga untuk meningkatkan efisiensi operasional perusahaan. Raymon Mcleod, Jr dan George P. Schell menyatakan bahwa "Sistem Informasi Manajemen adalah sistem berbasis komputer yang menyediakan informasi kepada pengguna dengan kebutuhan yang sama. Sedangkan menurut Joel E.Ross. "Sistem Informasi Manajemen adalah suatu kelompok orang, seperangkat pedoman dan petunjuk, peralatan mengolah data (seperangkat elemen) memilih, menyimpan, mengolah, dan mengambil kembali data (mengoperasikan data dan barang) untuk mengurangi ketidakpastian pada pengambilan keputusan (mencari tujuan bersama) dengan menghasilkan informasi untuk manajer pada waktu mereka dapat menggunakannya dengan paling efisien (menghasilkan informasi menurut waktu rujukan)".[31]

Manajemen perbankan merupakan disiplin ilmu yang berfokus pada pengelolaan semua aktivitas bank agar dapat beroperasi dengan lebih efisien dalam mencapai tujuannya.[32] Serta mengendalikan bagaimana perbankan melalui aktivitas operasinya, menghimpun dana, dan mendistribusikan hutang piutang.[33] Penilaian terhadap faktor manajemen dalam menilai kesehatan bank dilakukan melalui evaluasi pengelolaan bank tersebut.[34]

[31] Yulia Djahir and Dewi Pratita, *Sistem Informasi Manajemen* (Yogyakarta: Deepublish (Grup Penerbit CV Budi Utama), 2014). h. 15-17

[32] Zaki, "Pengertian Manajemen Perbankan Adalah: Tahapan, Resiko," 2023.

[33] Administrasi Publik, "Manajemen Bank : Pengertian, Tujuan, Fungsi, Struktur, Dan Unsur - Unsur Dalam Manajemen Bank," 2023.

[34] Veithzal Rivai, Andria Permata Veithzal, and Ferry N Indroes, *Bank and Financial Institution Management* (Jakarta: PT RajaGrafindo Persada, Jakarta, 2007). h. 121

a. User Bank

Menurut Kamus Besar Bahasa Indonesia, istilah "*user*" merujuk pada seseorang yang menggunakan suatu sistem, umumnya merujuk pada manusia.[35]

Dunia teknologi dan internet, istilah "*user*" biasanya mengacu pada individu atau konsumen yang menggunakan produk atau layanan digital. Contohnya termasuk pengguna aplikasi, pengunjung situs web, atau pelanggan dari *platform daring*.

Konteks perbankan, pengguna layanan bank umumnya dikenal sebagai nasabah. Menurut Undang-Undang No. 10 Tahun 1998 tentang Pokok-Pokok Perbankan, pasal (1) menjelaskan bahwa nasabah adalah individu atau entitas yang memanfaatkan layanan bank. Sementara itu, nasabah penyimpan adalah mereka yang menempatkan dana di bank dalam bentuk simpanan, sesuai dengan perjanjian yang dibuat antara bank dan nasabah tersebut.[36]

Djaslim Saladin menyatakan bahwa nasabah adalah individu atau entitas yang memiliki rekening tabungan atau pinjaman di bank.[37] Pelanggan atau nasabah adalah individu atau entitas yang membeli atau menggunakan produk yang disediakan oleh bank. Terdapat beberapa kategori nasabah, yaitu:

1. Pasar Konsumen : Konsumen individu atau rumah tangga yang mengakses produk bank untuk kebutuhan pribadi, seperti tabungan dan deposito.
2. Pasar Industri : Organisasi yang memperoleh produk untuk digunakan dalam proses produksi mereka.

[35] Pintarnya, "User," 2023.

[36] Presiden Republik Indonesia, "Undang-Undang Republik Indonesia Nomor 10 Tahun 1998 Tentang Perubahan Atas Undang-Undang Nomor 7 Tahun 1992 Tentang Perbankan," *Lembaran Negara Republik Indonesia*, 1998, pasal 1 ayat 3.

[37] M.Nur Rianto Al Arif, *Dasar-Dasar Pemasaran Bank* (Jakarta: CV Rajawali, 1994).h. 125

3. Pasar Pemerintah : Badan pemerintah, termasuk departemen atau BUMN, yang membeli produk dari bank.

4. Pasar Reseller : Organisasi yang membeli barang dan jasa untuk dijual kembali dengan margin keuntungan.

5. Pasar Internasional : Pembeli dari luar negeri, mencakup individu, produsen, reseller, dan lembaga pemerintah asing.[38]

b. Sistem *Firewall* Bank

Perkembangan sistem keamanan perbankan saat ini menghadirkan berbagai lapisan perlindungan, seperti biometrik, *firewall*, dan sistem pencegahan intrusi. Tujuan dari validasi berlapis ini adalah untuk memastikan bahwa akses hanya diberikan kepada individu yang berwenang. Pembaruan dan pemantauan sistem keamanan yang rutin dilakukan memastikan data terlindungi dari pencurian dan serangan *malware*.[39]

Menurut Roji, *firewall* adalah suatu metode atau mekanisme yang diterapkan pada perangkat keras, perangkat lunak, atau sistem itu sendiri. Tujuannya adalah untuk melindungi jaringan pribadi dengan cara menyaring, membatasi, atau bahkan menolak beberapa atau seluruh koneksi dari segmen jaringan ke jaringan eksternal yang tidak termasuk dalam ruang lingkupnya.[40]

Firewall adalah sistem yang dirancang untuk menilai dan mengontrol akses yang dianggap aman, serta mencegah akses dari jaringan yang tidak aman. *Firewall* dapat berupa perangkat lunak (seperti program atau aplikasi) atau perangkat keras (alat khusus yang menjalankan program *firewall*). Perangkat ini sangat penting karena berfungsi sebagai penghalang

[38] Kasmir, *Pemasaran Bank*, Revisi (Jakarta: Kencana, 2004).h.82

[39] Biotika, "Manfaat Dan Contoh Penerapan Teknologi Informasi Dalam Dunia Perbankan," Biotika, 2021

[40] Singgih Arif Widodo, Alimuddin Yasin, And Khurotul Aeni, "Keamanan Jaringan Firewall Dan Ids" (Yogyakarta, 2015).

keamanan antara jaringan komputer eksternal dan internal, menyaring lalu lintas jaringan yang masuk dan keluar.[41]

Firewall pada komputer berfungsi sebagai pertahanan utama untuk mencegah berbagai jenis serangan peretasan ke dalam jaringan. Setiap peretas yang berusaha mengakses jaringan akan mencari port terbuka yang bisa dimanfaatkan. Dengan adanya firewall dalam sistem jaringan, diharapkan informasi penting dapat terlindungi dan manajemen lalu lintas akses, baik dari dalam maupun luar sistem, dapat dilakukan dengan baik. Ini bertujuan untuk meningkatkan kinerja semua komponen terkait, sehingga koneksi atau jaringan menjadi optimal dan memberikan manfaat bagi pengguna.

4. Tinjauan tentang Kepercayaan Nasabah

a. Pengertian Tentang Kepercayaan

Lau dan Lee, seperti yang diungkapkan oleh Fandy Tjiptono, berpendapat bahwa kepercayaan terhadap suatu merek adalah elemen penting dalam menciptakan loyalitas. Hal ini dikarenakan kepercayaan mencerminkan kesiapan konsumen untuk mengandalkan produk atau layanan dalam situasi yang berisiko, berdasarkan harapan bahwa produk atau layanan tersebut akan memberikan hasil yang memuaskan.[42] Keyakinan terhadap suatu produk atau layanan bisa dianggap sebagai indikator kualitas hubungan antara konsumen dan produk atau layanan tersebut. Beberapa perusahaan percaya bahwa untuk meraih kepercayaan konsumen, mereka cukup menghasilkan produk atau layanan yang berkualitas tinggi. Menurut Robbins, kepercayaan adalah harapan positif bahwa orang lain tidak akan bertindak dengan cara yang merugikan, baik melalui ucapan, tindakan, maupun kebijakan.[43]

---

[41] Andy Nova Wijaya, "Pengertian Dan Fungsi Firewall," 2014.

[42] Fandy Tjiptono, *Pemasaran Jasa: Prinsip, Penerapan Dan Penelitian* (Yogyakarta: Andi Offset, 2014).

[43] Stephen P Robbins and Timothy A Judge, *Perilaku Organisasi*, Jilid 2 (Jakarta: Salemba Empat, 2011).

Definisi tingkat kepercayaan menurut Singh dan Sirdeshmukh menyatakan bahwa “kepercayaan adalah hal yang mendasar dalam membangun dan memelihara hubungan dalam waktu jangka Panjang”. Kepercayaan juga dapat diartikan sebagai keyakinan individu dalam menjalin kerja sama dengan pihak lain, yang pada gilirannya menciptakan hubungan kerja sama yang positif dalam jangka waktu yang panjang.[44] Dari berbagai definisi yang ada, dapat disimpulkan bahwa kepercayaan merujuk pada kesediaan konsumen untuk memanfaatkan layanan sebuah perusahaan, karena mereka yakin bahwa perusahaan tersebut dapat diandalkan untuk memenuhi janji yang dibuat. Hal ini pada akhirnya akan membangun loyalitas konsumen.

b. Kepercayaan Dalam Presfektif Islam

Imam al-Qusairi menjelaskan bahwa istilah "*shadiq*", yang merujuk pada orang yang jujur, berasal dari kata "*sadiq*", yang berarti kejujuran. Istilah "*shiddiq*" merupakan bentuk penekanan dari "*sadiq*", menggambarkan seseorang yang unggul dalam kejujuran. Dengan demikian, dalam diri orang yang jujur terdapat nilai-nilai spiritual yang mencerminkan berbagai sikap moral yang baik.[45]

Perilaku yang jujur mencerminkan sikap bertanggung jawab atas tindakan yang dilakukan, yang dikenal sebagai integritas. Kejujuran dan integritas saling melengkapi, bagaikan dua sisi dari koin yang sama. Seseorang tidak hanya perlu memiliki keikhlasan dan kejujuran, tetapi juga harus dilengkapi dengan nilai-nilai lain yang mendorongnya, seperti integritas. Hal ini membuat individu tersebut siap menghadapi risiko dan konsekuensi dengan berani, penuh kebanggaan, dan sukacita, tanpa pernah berpikir untuk melemparkan tanggung jawab kepada orang lain. Dalam Islam, Q.S. Ali

[44] elibrary.unikom.ac.id
[45] K.H. Toto Tasmara, *Membudayakan Etos Kerja Islam* (Jakarta: Gema Insani, 2002).80

Imran/3:159 mengajarkan kepada orang-orang beriman, khususnya pelaku usaha, untuk bersikap lembut dan memuaskan dalam dakwah mereka.

﴿ فَبِمَا رَحْمَةٍ مِّنَ اللّٰهِ لِنْتَ لَهُمْ ۚ وَلَوْ كُنْتَ فَظًّا غَلِيْظَ الْقَلْبِ لَانْفَضُّوْا مِنْ حَوْلِكَ ۖ
فَاعْفُ عَنْهُمْ وَاسْتَغْفِرْ لَهُمْ وَشَاوِرْهُمْ فِى الْاَمْرِ ۚ فَاِذَا عَزَمْتَ فَتَوَكَّلْ عَلَى اللّٰهِ ۗ اِنَّ اللّٰهَ
يُحِبُّ الْمُتَوَكِّلِيْنَ ﴿١٥٩﴾ ﴾

Terjemahnya :

> Dengan izin Allah, engkau (Nabi Muhammad) menunjukkan sikap lemah lembut kepada mereka. Jika engkau bersikap keras dan kasar, mereka pasti akan menjauh darimu. Oleh karena itu, maafkanlah mereka, mintalah ampunan untuk mereka, dan lakukan musyawarah dalam hal-hal penting. Setelah engkau membuat keputusan, percayalah kepada Allah. Sesungguhnya, Allah menyukai orang-orang yang berserah diri kepada-Nya.[46]

Artinya adalah: segala hal yang berkaitan dengan perang dan berbagai aspek duniawi lainnya, termasuk politik, ekonomi, dan masalah sosial.

Morgan dan Hunt menunjukkan bahwa kepercayaan adalah fondasi penting untuk kolaborasi antar perusahaan. Temuan serupa juga diungkapkan oleh Ganesan, yang menyatakan bahwa kepercayaan berpengaruh pada niat untuk mempertahankan hubungan jangka panjang. Menurut Morgan dan Hunt, ada beberapa keuntungan dari kepercayaan, yaitu:

1) Kepercayaan mendorong pemasar untuk berusaha menjaga hubungan yang telah terjalin dengan mitra dagang.

[46] Kementerian Agama RI, "Al-Qur'an Dan Terjemahahnnya," Q.S. Ali-imran, 159

2) Kepercayaan mengarahkan pada penghindaran pilihan jangka pendek dan lebih fokus pada keuntungan jangka panjang, yaitu mempertahankan mitra yang ada.
3) Kepercayaan dapat membantu pemasar mengambil keputusan yang lebih bijak dalam menghadapi risiko besar, karena mitra tidak akan memanfaatkan situasi yang dapat merugikan pemasar.[47]

c. Teori Kepercayaan Nasabah

Menurut Sumarwan dalam Sangadji & Sopiah kepercayaan nasabah dapat didefinisikan sebagai keyakinan bahwa suatu produk memiliki karakteristik tertentu. Hal ini sering disebut sebagai keterkaitan antara objek dan atribut, yang merujuk pada kepercayaan konsumen mengenai potensi hubungan antara sebuah objek dan atribut yang relevan'.

Menurut Mowen & Minor, kepercayaan merujuk pada pengetahuan yang dimiliki konsumen tentang objek, atribut, dan manfaatnya. Sementara itu, McKnight et al. menjelaskan bahwa kepercayaan tumbuh antara pihak yang belum saling mengenal baik dalam interaksi atau proses transaksi. Dalam konteks ini, dua aspek utama dari kepercayaan konsumen yaitu:[48]

1) Keyakinan Mempercayai (*Trusting Belief*)

Trusting belief merujuk pada tingkat kepercayaan seseorang terhadap pihak lain dalam konteks tertentu. Ini merupakan persepsi konsumen terhadap perusahaan atau pemasar, di mana perusahaan dianggap memiliki karakteristik yang menguntungkan bagi konsumen. Tiga elemen utama yang membangun trusting belief adalah niat baik, integritas, dan kompetensi.

[47] Mulyo Budi Setiawan and Ukudi Ukudi, "Pengaruh Kualitas Layanan, Kepercayaan Dan Komitmen Terhadap Loyalitas Nasabah (Studi Pada Pd. Bpr Bank Pasar Kendal)," *Jurnal Bisnis Dan Ekonomi (JBE), September 2007, Hal. 215-227 Vol.14, No.2* 14, no. 2 (2007): 215–27.

[48] Wijanarko et al., "Analisis Dan Simulasi Serangan *Ransomware* Terhadap Database Bank Syariah Indonesia."

a) Niat Baik (*Benevolence*)

Mengacu pada seberapa besar kepercayaan konsumen kepada penjual dalam berperilaku positif. *Benevolence* mencerminkan kesediaan penjual untuk melayani kepentingan konsumen secara berkelanjutan.

b) Integritas (*Integrity*)

Berkaitan dengan keyakinan konsumen terhadap kejujuran penjual dalam memenuhi kesepakatan yang ada.

c) Kompetensi (*Competence*)

Merupakan keyakinan terhadap kemampuan penjual dalam membantu konsumen memenuhi kebutuhannya. Kompetensi menunjukkan seberapa efektif penjual dalam mencapai hasil yang diinginkan konsumen.

2) Niat untuk Mempercayai (*Trusting Intention*)

Trusting intention adalah keputusan sadar di mana seseorang bersedia bergantung pada orang lain dalam situasi tertentu. McKnight et al. menjelaskan bahwa ada dua elemen yang mendasari trusting intention, yaitu kesediaan untuk bergantung dan probabilitas subjektif untuk bergantung.

a) Kesediaan untuk Bergantung (*Willingness to Depend*)

Merujuk pada kesiapan konsumen untuk bergantung pada penjual dengan menerima risiko atau konsekuensi yang mungkin timbul.

b) Probabilitas Subjektif untuk Bergantung (*Subjective Probability of Depending*)

Mengacu pada kesediaan konsumen secara subjektif untuk memberikan informasi pribadi, melakukan transaksi, dan mengikuti saran atau permintaan dari penjual.

d. Faktor-faktor Yang Mempengaruhi Kepercayaan

Ada beberapa faktor yang memengaruhi kepercayaan seseorang, yaitu:

1) Reputasi adalah karakteristik yang diberikan kepada penjual berdasarkan informasi dari individu atau sumber lain. Reputasi memainkan peran penting dalam membangun kepercayaan konsumen terhadap penjual, terutama ketika konsumen tidak memiliki pengalaman pribadi. Informasi positif yang disebarkan dari mulut ke mulut dapat menarik minat konsumen. Ketika konsumen menerima informasi yang baik tentang penjual, hal ini dapat mengurangi persepsi risiko dan ketidakamanan saat melakukan transaksi.
2) *Perccived quality* yaitu persepsi akan kualitas baik itu dari segi produk, pelayan maupun pengahargaan. Tampilan serta desain perusahaan juga dapat mempengaruhi kesan pertama yang terbentuk.[49]

e. Strategi Membangun Kepercayaan Pelanggan

Berikut adalah parafrase dari teks yang Anda berikan:

1) Tentukan Standar Kualitas

Tentukan standar kualitas yang jelas untuk setiap produk atau layanan yang ditawarkan. Hindari pengurangan kualitas; sebaliknya, upayakan untuk terus meningkatkan kualitas tersebut. Dengan demikian, kepercayaan pelanggan akan terbangun.

[49] DEwi Intan Kusuma, "Pengaruh Kepercayaan Terhadap Loyalitas Konsumen Pada Bedak My Baby (Studi Pada Siswi SMKN2 Kediri Kelas XI)," *Skripsi Iain Kediri*, 2021, 21–33.

2) Tingkatkan Komunikasi dan Interaksi

Menciptakan pengalaman positif bagi pelanggan sangat bergantung pada komunikasi dan interaksi yang efektif. Pastikan untuk berkomunikasi dengan baik dan memberikan solusi yang sesuai dengan kebutuhan pelanggan. Respon yang cepat terhadap permintaan konsumen akan memperkuat hubungan, terutama bagi mereka yang memerlukan bantuan atau informasi.

3) Berikan Kesan Pertama yang Positif

Salah satu cara untuk membangun kepercayaan pelanggan adalah dengan menunjukkan nilai-nilai perusahaan Anda dan memberikan kesan pertama yang baik. Usahakan bisnis Anda meninggalkan impresi yang positif agar pelanggan dapat mempercayai Anda di masa mendatang. Selalu pastikan produk dan layanan Anda berkualitas, dimulai dengan mengkomunikasikan nilai-nilai perusahaan dan mengambil tindakan yang mencerminkannya. Ini akan membuat bisnis Anda terlihat lebih otentik dan meningkatkan kepercayaan pelanggan.

4) Pengumpulan Umpan Balik

Kumpulkan saran dan kritik melalui pertemuan langsung, survei via email, atau survei pop-up di situs web Anda. Umpan balik dari pelanggan dapat membantu Anda melakukan perbaikan yang diperlukan untuk produk dan layanan.

5) Apresiasi Pelanggan

Untuk menjaga loyalitas pelanggan, pertimbangkan untuk memberikan poin pada setiap pembelian yang dapat ditukarkan dengan produk Anda. Ini dapat meningkatkan keterlibatan pelanggan di masa depan dan mendorong mereka menjadi pelanggan setia.

6) Kenyamanan dan Keamanan Transaksi

Nasabah harus merasa nyaman saat bertransaksi, baik di dalam maupun di luar bank. Mereka tidak seharusnya merasa khawatir saat berinteraksi dengan bank.

7) Penanganan Keluhan

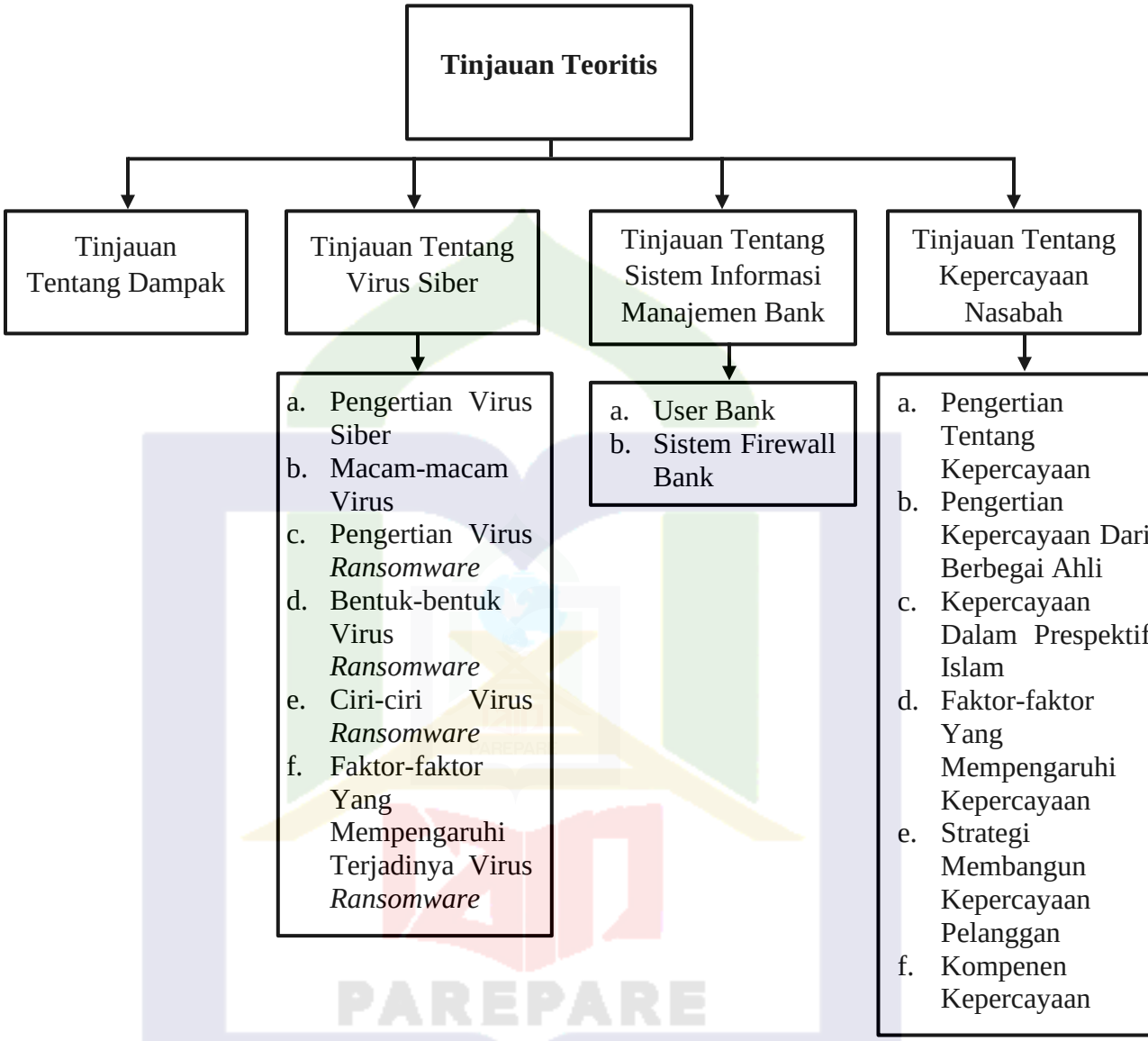
Setiap keluhan atau komplain dari nasabah harus ditanggapi dengan cepat dan efektif.[50]

f. Komponen Kepercayaan

1) Kepercayaan dapat diartikan sebagai kesiapan untuk mengandalkan mitra dalam pertukaran yang dipercaya. Menurut Green, seperti yang dikutip oleh *Fasochah*, ada beberapa komponen utama dari kepercayaan:1. Kredibilitas: Ini mencakup kejujuran karyawan dan kepercayaan terhadap ucapan mereka. Kredibilitas harus dibuktikan dengan pernyataan, seperti, "Saya dapat mempercayai apa yang dikatakannya tentang..." Istilah terkait lainnya adalah kepercayaan dan kebenaran.
2) Reabilitas : Merujuk pada kemampuan untuk diandalkan. Ini berhubungan dengan kualitas individu atau organisasi. Keandalan harus dibuktikan melalui tindakan, seperti, "Saya dapat mempercayai apa yang dilakukannya..." Istilah lain yang berkaitan adalah kepastian dan keterkenalan.
3) *Intimacy* : Terkait dengan integritas, yang berarti karyawan memiliki prinsip moral yang kuat. Integritas mencerminkan konsistensi internal, di mana ada kesesuaian antara ucapan dan tindakan serta antara pikiran dan tindakan. Selain itu, integritas juga mencerminkan ketulusan.[51]

[50] https://sisi.id.

[51] Fasochah and Harnoto, "Analisis Pengaruh Kepercayaan Dan Kualitas Layanan Terhadap Loyalitas Pelanggan Dengan Kepuasan Konsumen Sebagai Variabel Mediasi (Studi Pada RS Darul



Gambar 2.1.

Tinjauan Teoritis

Istiqomah Kaliwungu Kendal) Hartono," *Jurnal Ekonomi Manajemen Akuntansi* 20, no. 34 (2013): 1–14.

C. Tinjauan Konseptual

Dari tinjauan teori ada beberapa istilah-istilah yang perlu penulis konsep lebih rinci agar memudahkan memberikan gambaran dalam objek penelitian, istilah-istilah dalam penelitian ini, yaitu :

1. Dampak

   Dampak merujuk pada perubahan yang terjadi sebagai hasil dari aktivitas atau tindakan yang telah dilakukan sebelumnya. Ini merupakan konsekuensi dari penerapan suatu kebijakan, yang dapat menghasilkan perubahan yang bersifat positif maupun negatif.

2. Bank Syariah

   Bank Islam atau selanjutnya disebut bank syariah nampaknya sudah tidak asing bagi masyarakat Indonesia pada umumnya. Bank syariah merupakan salah satu lembaga keuangan bank yang beroperasi sebagai lembaga keuangan yang menyediakan layanan jasa keuangan atau transaksi kepada nasabahnya. Adanya penyebutan sebagai perbankan syariah karena sistem operasional keuangan yang dijalankannya tidak terlepas dari prinsi-prinsip Islam.[52] Adapun Bank Syariah adalah lembaga keuangan yang operasionalnya berlandaskan pada prinsip-prinsip hukum Islam, di mana bank ini tidak mengenakan bunga maupun memberikan bunga kepada nasabah.[53]

3. Manajemen Bank Syariah

   Manajemen bank syariah berfungsi sebagai lembaga yang mengumpulkan dana dari masyarakat untuk pembiayaan dan menjalin hubungan keuangan dengan pihak bank. Struktur manajemen bank mencakup dua elemen utama:

---

[52] I Nyoman Budiono, *Manajemen Pemasaran Bank Syariah*, ed. Asriadi Arifin (Parepare: IAIN Parepare Nusantara Press, 2022).

[53] Ivalaina Astarina and Angga Hapsila, *Manajemen Perbankan*, ed. Puspa Dewi and Syafrizal, *Deepublish (Grup Penerbit CV Budi Utama)*, 1st ed. (Yogyakarta: Deepublish (Grup Penerbit CV Budi Utama), 2015).

manajemen umum dan manajemen risiko. Setiap elemen akan dinilai berdasarkan kesehatan bank dari perspektif manajerial.[54]

4. Kepercayaan Nasabah

Kepercayaan nasabah merupakan sikap dan perilaku yang perlu dijaga oleh pihak yang berkaitan dengan konsumen dalam dunia perbankan, dilihat dari layanan, manfaat serta hasil yang diberikan sesuai kemauan nasabah.

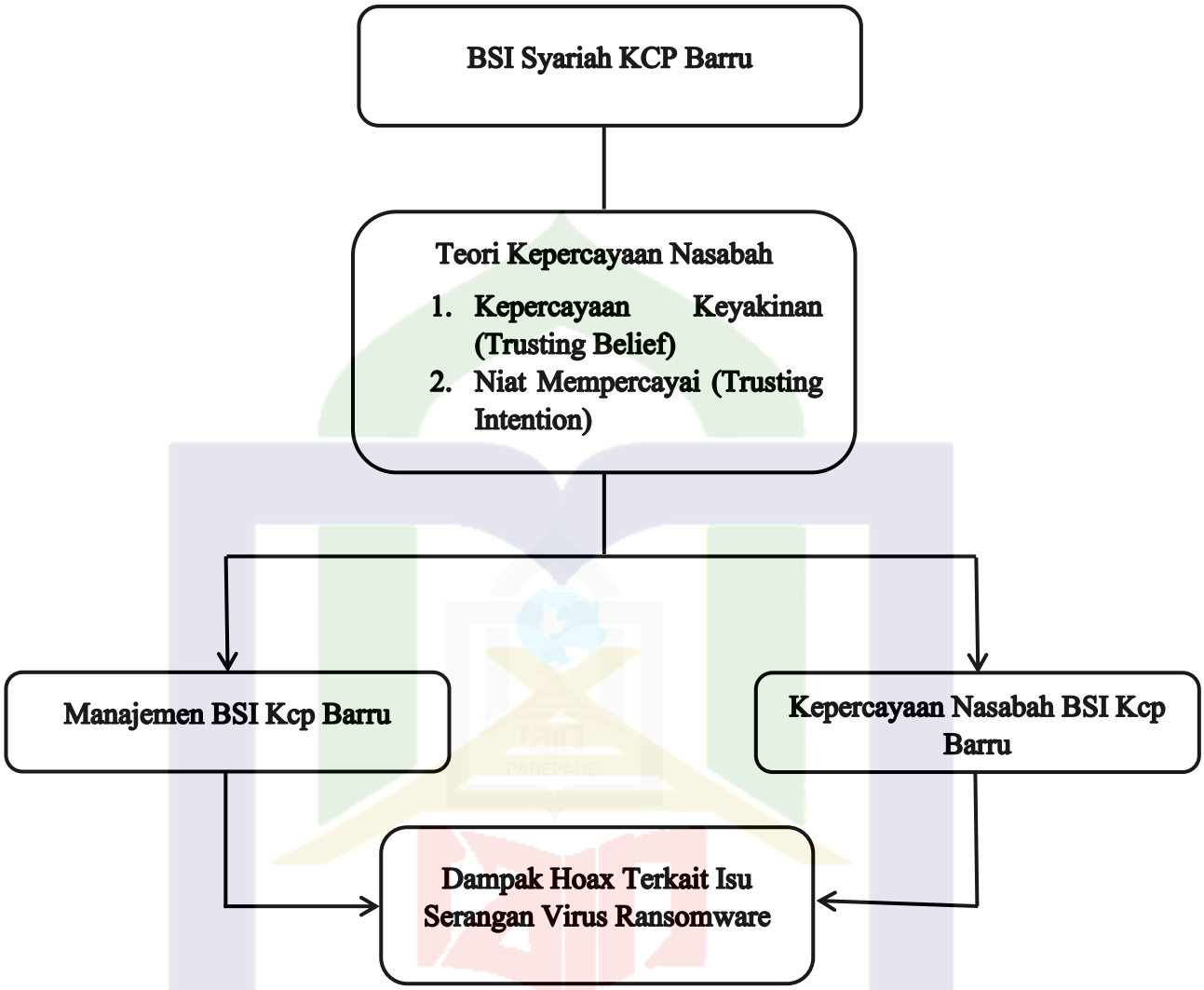
5. Virus *Ransomware*

Berdasarkan tinjauan teoritis dapat disimpulkan bahwa virus *ransomware* adalah Virus *ransomware* salah satu jenis dari virus *malware* yang menyerang sistem perangkat bank berupa mengenkripsi data dan perangkat penting, virus ini bersifat menyebar ke seluruh jaringan dengan menargetkan database dan server file dengan instan.

D. Kerangka Pikir

Kerangka pikir adalah representasi atau penjelasan sementara mengenai fenomena yang menjadi fokus permasalahan. Dalam hal ini, kerangka pikir digunakan untuk mengevaluasi tingkat kepuasan nasabah BSI terkait dampak dari serangan virus *Ransomware* terhadap penyimpanan dana. Di bawah ini adalah ilustrasi bagan kerangka pikir tersebut:

[54] I Wayan Sudirman, *Manajemen Perbankan,* ed. Riefmanto, 1st ed. (Jakarta: Kencana, Prenada Media Group, 2013).



Gambar 2.2 : Bagan Kerangka Pikir

BAB III

METODE PENELITIAN

A. Pendekatan dan Jenis Penelitian

Pendekatan yang diterapkan dalam penelitian kualitatif ini adalah studi kasus, yang berfokus pada analisis mendalam terhadap suatu fenomena atau kejadian spesifik dalam masyarakat. Tujuan dari pendekatan ini adalah untuk memahami konteks, kondisi, dan interaksi yang berlangsung. Studi kasus dapat mencakup suatu sistem, seperti program, kegiatan, peristiwa, atau sekelompok individu dalam situasi tertentu.[55] Tipe penelitian ini adalah penelitian deskriptif, yang berarti fokusnya adalah untuk menggambarkan fenomena, peristiwa, atau kejadian yang terjadi saat ini. Penelitian deskriptif menyoroti isu-isu terkini sebagaimana adanya selama proses penelitian. Dalam konteks ini, peneliti berusaha untuk menggambarkan dampak serangan virus *ransomware* terhadap kepercayaan nasabah dalam menyimpan dana di BSI Kcp Barru.

B. Lokasi dan Waktu Penelitian

1. Lokasi Penelitian

   Penelitian ini dilaksanakan di PT Bank Syariah Indonesia, yang berlokasi di Perum. Griya UBM Blok A.5, Jl. A.A Bau Massepe Ling., Kabupaten Barru. Penulis memilih lokasi ini karena memiliki pengalaman magang selama 5 bulan dalam program MBKM (Merdeka Belajar Kampus Merdeka), yang memberikan keuntungan tersendiri dalam pelaksanaan penelitian.

2. Waktu Penelitian

   Penelitian ini dilaksanakan dalam jangka waktu dua bulan.

C. Fokus Penelitian

Studi ini menyoroti dampak adanya virus *ransomware* terhadap tingkat kepercayaan nasabah di BSI KCP Barru.

---

[55] Muhammad Kamal Zubair, *Penulisan Karya Ilmiah Berbasis Teknologi Informasi*, Terbaru (Parepare, 2021).

D. Jenis dan Sumber Data

Sumber data yang penulis gunakan dalam penelitian ini adalah data primer dan data sekunder.

1. Data Primer

Data primer merujuk pada informasi yang diperoleh secara langsung dari subjek, baik melalui komunikasi verbal, tindakan, atau perilaku yang dapat dipercaya, dalam konteks variabel yang sedang diteliti. Dalam penelitian ini, sumber data primer terdiri dari informasi yang dikumpulkan langsung dari pihak yang mengalami masalah dengan transaksi ATM yang telah terjadi beberapa kali. Dampak dari serangan virus *ransomware* telah mengganggu sistem informasi bank, sehingga menimbulkan kecemasan di kalangan nasabah mengenai keamanan tabungan mereka. Beberapa nasabah akan diwawancarai untuk mendalami isu ini di BSI KCP Barru.

2. Data Sekunder

Data sekunder adalah informasi yang diambil dari sumber asal yang menyediakan data relevan untuk penelitian ini, seperti artikel, majalah, jurnal, dan situs web.

E. Teknik Pengumpulan Data

Teknik pengumpulan data yang diterapkan dalam penelitian ini meliputi:

1. Observasi

Observasi adalah metode pengumpulan data yang berbeda dari wawancara dan kuesioner. Teknik ini tidak hanya berfokus pada individu, tetapi juga pada objek tertentu. Dengan kata lain, observasi, atau yang juga dikenal sebagai pengamatan, mencakup proses memusatkan perhatian pada suatu objek dengan memanfaatkan indera.

2. Wawancara

Dalam penelitian kualitatif, sumber data utama biasanya adalah manusia yang berperan sebagai informan. Oleh karena itu, wawancara mendalam menjadi metode utama untuk menggali informasi, memungkinkan peneliti untuk memperoleh data yang lebih kaya, komprehensif, dan mendalam.

3. Dokumentasi

Dokumentasi adalah salah satu metode untuk mengumpulkan data, menghasilkan catatan atau informasi penting yang relevan dengan penelitian. Data yang diperoleh melalui dokumentasi dianggap sah dan dapat dijadikan rujukan karena tidak berdasarkan asumsi.

F. Uji Keabsahan Data

Keabsahan data merujuk pada kesesuaian antara informasi yang diperoleh peneliti dan keadaan sebenarnya dari objek penelitian, sehingga hasil yang disajikan dapat dipertanggungjawabkan. Dalam penelitian kualitatif, uji keabsahan data mencakup credibility, transferability, dependability, dan confirmability.

G. Teknik Analisis Data

1. Pengurangan Data

Pengurangan data merujuk pada proses merangkum dan memilih elemen-elemen utama, dengan fokus pada hal-hal penting, sambil mengeliminasi informasi yang tidak relevan. Tujuannya adalah untuk menghasilkan ringkasan inti dari data yang diperoleh.

2. Presentasi Data

Dalam penelitian kualitatif, data yang dikumpulkan umumnya berbentuk naratif. Oleh karena itu, penting untuk menyajikan data dengan cara yang menyederhanakan tanpa mengurangi makna, sehingga informasi terstruktur dengan baik dan memungkinkan penarikan kesimpulan.

3. Kesimpulan

Kesimpulan atau verifikasi adalah langkah terakhir dalam analisis data, di mana peneliti menyampaikan hasil dari data yang telah dikumpulkan.diperoleh.

BAB IV

HASIL PENELITIAN DAN PEMBAHASAN

A. Hasil Penelitian

1. Bentuk serangan virus *ransomware* terhadap Bank Syariah Indonesia (BSI) di Kcp Barru

Jenis serangan siber yang menarget Bank Syariah Indonesia diduga adalah serangan *malware*. *Malware* adalah perangkat lunak yang sengaja dibuat untuk merusak komputer atau jaringan komputer. Serangan ini adalah salah satu yang paling umum ditemui dalam sistem IT perusahaan. *Malware* dapat menyerang file seseorang dan menggandakan diri, merusak sistem kerja harddisk dan perangkat lunak, mencuri data, serta merusak sistem informasi pada komputer target. Selain *malware*, ada juga *ransomware* yang sangat merugikan dan berbahaya. *Ransomware* dapat merusak sistem perangkat hingga tidak dapat dioperasikan dan memiliki kemampuan untuk menyebar dan menginfeksi perangkat lain di sekitarnya.

Berbeda dengan isu yang diberitakan mengenai serangan tersebut, pihak dari BSI Kcp Barru sendiri membantah adanya serangan siber *malware* yang menyerang Bank Syariah Indonesia ia menyatakan bahwa hal tersebut merupakan isu yang dibuat untuk merusak nama baik Bank Syariah Indonesia. Sebagaimana ia mengatakan hal tersebut melalui wawancara dengan peneliti di bawah ini:

> "Intinya Alhamdulillah kemarin tidak ada satupun nasabah yang hilang dananya semuanya aman." Beliau melanjutkan, "kalaupun ada isu yang bahwa dananya hilang dan itu hanya orang tertentu yang di bayar untuk menghancurkan nama baik BSI karna kita tau isu yang diberitakan tentang sekelompok penyerangan siber yang dinamai virus *malware* merupakan hanya sebuah gertakan yang di berikan untuk menantang pihak Bank Syariah Indonesia."[56]

[56] Amiruddin, BOSM, wawancara oleh penulis di BSI Kcp Barru, 24 April 2024.

Dari hasil wawancara di atas Bank Syariah berani memberikan jaminan bahwa data-data semua nasabah aman dan tersimpan rapi bahkan tidak bocor akibat isu maupun gertakan dari isu siber. Hal ini juga diperkuat oleh *customer service* BSI Kcp Barru yang menjadi narasumber yaitu Bapak Ardiansya, beliau menuturkan bahwa:

> "Pada saat hal ini terjadi jaringan belum stabil, terkadang jaringan off di siang hari tapi bisa ji di malam hari di gunakan. Sampai-sampai pegawai yang tadinya mau mengimput di siang hari tidak bisa, jadi mereka mengimputnya di malam hari."[57]

Ini menunjukkan bahwa serangan siber hanyalah ancaman yang dihasilkan oleh grup penyerang siber LockBit 3.0, yang menggunakan metode phishing dan lampiran berbahaya untuk menyebarkan *ransomware* ke dalam sistem perbankan, dimana isu tersebut membawa dampak besar bagi Bank Syariah Indonesia yang mengakibatkan sebagian dari nasabah BSI mulai menarik dananya sehingga berdampak cukup signifikan dari yang semestinya. Selain itu, fakta yang beredar bahwa masalah yang terjadi di BSI bukan dikarenakan isu siber melainkan adanya kerusakan server IT yang bermasalah dari kantor pusat hingga merambat ke semua server di kantor-kantor cabang Bank Syariah Indonesia mengalami error.

Sebagaimana pernyataan dari *Branch Operation Service Manager* (BOSM) yaitu sebagai berikut :

> "Karena kemarin adanya 3 bank yang di gabungkan menjadi satu otomatis server yang ada pada 3 bank tersebut tidak dapat membendung kapasitas banyaknya nasabah yang ada. Makanya memerlukan server tambahan, proses penambahan server inilah yang membuat error jaringan sehingga mengakibatkan pemindahan server yang memakan waktu sampai 6 hari dan itu yang tidak dipahami nasabah Banyaknya isu yang berkembang, jadi hackerlah itu Cuma isu-isu ini saja padahal untuk lebih meningkatkan keamanan cybernya data nasabah maka perlu penambahan satu server di kantor pusat."[58]

[57] Ardiansya, *customer service*, wawancara oleh penulis di BSI Kcp Barru, 24 April 2024.
[58] Amiruddin, BOSM, wawancara oleh penulis di BSI Kcp Barru, 24 April 2024.

Dari hasil wawancara tersebut, dapat disimpulkan bahwa kurangnya kapasitas server IT Bank Syariah Indonesia membuat jaringan server yang mengalami error sehingga tidak dapat melakukan transaksi baik secara online, seperti BSI mobile, transaksi melalui ATM, maupun transaksi offline yang dilakukan di Bank Syariah Indonesia belum lagi dari bank lain yang memanfaatkan situasi yang terjadi karena hal ini sangat mempengaruhi nasabah.

Peneliti melanjutkan wawancara terkait hal tersebut dengan *customer service* BSI Kcp Barru yaitu Pak Ardiansya, beliau menuturkan bahwa:

> "Pada saat itu terjadi kita tidak bisa apa-apa, seperti transaksi BSI mobile maupun online tidak bisa dilakukan. Transaksi terjadi war seluruh cabang mengadu ke kantor pusat dikarenakan hal tersebut."[59]

Dari wawancara di atas dapat diambil kesimpulan bahwa sebagaimana yang di beritakan serangan virus *ransomware* yang merupakan salah satu jenis dari virus *malware* mulai menyerang sistem IT di kantor pusat BSI hal tersebut membuat keamanana sistem BSI mengalami error hingga membuat transasksi di seluruh kantor cabang BSI tidak bisa dilakukan. Sebagaimana tanggapan dari pihak BSI Kcp Barru mengatakan hal tersebut merupakan hoax isu yang di buat oleh sekelompok orang-orang tertentu untuk merusak nama baik bank syariah indonesia, faktanya hal ini tidak pernah terjadi dan masih menjadi dugaan yang tidak berdasar sebagaimana yang diberitakan. Terjadinya hal tersebut dikarenakan kelalaian dari manajemen IT di kantor pusat BSI akibatnya server IT BSI mengalami error selama beberapa hari ini.

2. Dampak serangan yang di duga virus *ransomware* terhadap kepercayaan nasabah Bank Syariah Indonesia (BSI) di Kcp Barru

Serangan *ransomware* terhadap Bank Syariah Indonesia (BSI) memiliki dampak yang signifikan, tidak hanya mengganggu operasional internal bank,

[59] Ardiansya, *customer service*, wawancara oleh penulis di BSI Kcp Barru, 24 April 2024.

tetapi juga berpotensi merusak kepercayaan nasabah terhadap sistem perbankan dan keamanan data mereka.

Bukti lebih lanjut diperoleh dari wawancara dengan Bapak Ardiansya, customer service BSI Kcp Barru, di mana beliau menjawab pertanyaan mengenai dampak serangan virus *ransomware* terhadap kepercayaan nasabah dengan penjelasan berikut :

> "Berpengaruh contohnya karena kan namanya ada serangan pasti terganggu sistem pasti nasabah tidak bisa bertransaksi kalau nasabah tidak bisa bertransaksi pasti tidak nyaman akhirnya itu bisa menurunkan kepercayaan nasabah karena uangnya merasa terganggu."[60]

Sebagaimana wawancara di atas menjelaskan bahwa serangan virus *ransomware* sangat berpengaruh dan memiliki dampak yang besar kepada nasabah. Selain itu pertanyaan tersebut dapat diperkuat dengan wawancara yang dilakukan oleh peneliti dengan Bapak Branch Operation Service Manager (BOSM) Bank Syariah Indonesia (BSI) Kcp Barru melalui serangkaian pertanyaan. pertanyaan, Bagaimana dampak yang di sebabkan serangan virus *ransomware* di BSI Kcp Barru ?

> "Terjadi penurunan nasabah dan mengalami larinya nasabah mulai dari nasabah besar atau nabasah prioritas pindah, belum lagi dari bank lain yang memanfaatkan keadaan tersebut. Istilahnya ada dari pihak internal dan ada dari pihak eksternal."[61]

Berdasarkan dari wawancara diatas bahwa diketahui Bank Syariah Indonesia Kcp Barru mengalami penurunan nasabah dan menarik dana dari bank BSI dikarenakan dampak dari kejadian tersebut ujar salah satu nasabah Bank Syariah Indonesia menuturkan bahwa :

[60] Ardiansya, *customer service*, wawancara oleh penulis di BSI Kcp Barru, 24 April 2024.
[61] Amiruddin, BOSM, wawancara oleh penulis di BSI Kcp Barru, 24 April 2024.

"BSI masih belum bisa menerima transferan dari bank lain, jalan lain saya tarik semua dana di bank BSI dan tutup rekening disana. Waktunya pindah ke bank lain yang lebih berkualitas. Itu satu-satunya cara untuk menyelamatkan dana yang saya punya."[62]

Tidak hanya itu, semua tugas di BSI mengalami gangguan, sebagaimana dijelaskan oleh Branch Operation Service Manager (BOSM) Bank Syariah Indonesia (BSI) Kcp Barru, beliau menyatakan bahwa:

> "Seluruh jobdesk mulai dari OB sampai pimpinan sampai jajaran direksi, direktur utama BSI kenna semua, kita kekantor hanya istilahnya pasang badan dan permohonan sama nasabah, minta maaf itu saja kita lakukan selama satu minggu, mau ki kerja tidak bisa online server karena semua pekerjaan perbankan itu online ketika server perbankan rusak maka terganggu semua mi itu."[63]

Sesuai dengan apa yang telah disampaikan di atas menginformasikan seluruh jobdesk Bank Syariah Indonesia di Kcp Barru terganggu diakibatkan jaringan server mengalami error dan tidak bisa diakses sama sekali hal ini mengganggu transaksi yang dilakukan. Wawancara lain yang disampaikan customer service BSI Kcp Barru mengenai jobdesk tersebut, sebagai berikut:

> "Semua jobdesk BSI Kcp Barru mengalami gangguan mulai dari layanan gadai, *costumer service, teller* tidak bisa beroperasi. Mobile banking juga begitupun dengan ATM."[64]

Penjelasan di atas bahwa BSI Kcp Barru bahkan transaksi yang biasanya terjadi juga mengalami gangguan. Peneliti melanjutkan wawancara terkait dampak serangan yang virus *ransomware* kepada bapak Branch Operation Service Manager (BOSM) yaitu sebagai berikut :

> "Tidak ada transaksi apapun mau BSI Mobile, mau transaksi teller, cs, internet banking pokoknya apapun terkait BSI kemarin tidak ada yang bisa diakses sama sekali. Namanya transaksi online, online kan

[62] Hamzah *nasabah,* wawancara oleh penulis di BSI Kcp Barru, 24 April 2024
[63] Amiruddin, BOSM, wawancara oleh penulis di BSI Kcp Barru, 24 April 2024.
[64] Ardiansya, *customer service,* wawancara oleh penulis di BSI Kcp Barru, 24 April 2024.

> transaksinya semua dari server, nah server ini yang bermasalah dan tidak ada apapun yang bisa, mau perbaiki pun tidak bisa, buka rekening tidak bisa, setor uang tidak bisa, penarikan apalagi, mau lewat ATM nasabah juga tidak bisa karena error ki ATM mau lewat BSI mobile, transfer ke bank lain tidak bisa, error ki BSI mobile, pokoknya hancur tidak ada semua yang bisa dilakukan."[65]

Sebagaimana dari hasil wawancara di atas, sulitnya transaksi di bank, melalui mobile banking hingga melalui ATM tidak bisa dilakukan. Dapat dilihat dari penjelasan bagaimana dampak yang diberikan cukup mempengaruhi pihak bank. Selanjutnya, peneliti melanjutkan wawancara terkait dampak virus *ransomware* terhadap nasabah Bank Syariah Indonesia kepada Julianti (nasabah) mengatakan bahwa :

> "Ada kendalanya, tidak bisa ki melakukan penarikan di ATM, bahkan transaskis QRIS di BSI *mobile* juga mengalami gangguan. Intinya saat saya butuh transaksi, maumi di apa kalo ada masalah yang terjadi pada ATMnya."[66]

Wawancara yang dilakukan oleh peneliti di atas menunjukkan bahwa hal tersebut langsung memberikan dampak pada nasabah yang ingin melakukan transaksi, ini juga memperkuat wawancara yang dilakukan oleh peneliti pada *Branch Operation Service Manager* (BOSM) maupun teller Bank Syariah Indonesia.

Berdasarkan dari wawancara diatas dapat disimpulkan bahwa bank Syariah Indonesia Kcp Barru mengalami dampak yang sangat besar dari serangan yang di duga virus *ransomware*, adanya dari pihak internal dan dari pihak eksternal. Hal ini berdampak pada kepercayaan nasabah sehingga mengalami penurunan, mulai dari nasabah besar maupun nasabah prioritas menarik dananya selain itu adanya bank-bank lain yang memanfaatkan keadaan

[65] Amiruddin, BOSM, wawancara oleh penulis di BSI Kcp Barru, 24 April 2024.
[66] Julianti *nasabah*, wawancara oleh penulis di Lapakaka, 25 April 2024.

tersebut. Bahkan seluruh jobdesk yang ada di Bank Syariah Indonesia Kcp Barru juga terkena dampaknya dikarenakan hal itu transaksi dan pengimputan data online maupun offline harus di tunda hingga jaringan server kembali normal, intinya pihak bank tidak banyak yang bisa mereka lakukan di tengah-tengah masalah yang terjadi.

3. Upaya Bank Syariah Indonesia (BSI) di Kcp Barru dalam memulihkan kepercayaan nasabah setelah terjadinya serangan virus *ransomware*

Kasus Bank Syariah Indonesia (BSI) adalah contoh jelas yang menunjukkan pentingnya langkah serius dalam menghadapi serangan *ransomware*. Keamanan digital harus menjadi prioritas utama bagi lembaga keuangan dan organisasi lainnya untuk melindungi data dan sistem mereka dari serangan yang merugikan dan berbahaya.

Sebagaimana dari hasil wawancara peneliti terkait upaya Bank Syariah Indonesia di Kcp Barru dalam menangani keluhan nasabah terhadap layanan error, hal ini akan di jawab oleh pak Emir selaku Branch Operation Service Manager (BOSM), beliau menuturkan bahwa:

> "Langkah awal yang dilakukan Bank Syariah Indonesia Kcp Barru, seperti melakukan pendekatan spritual kita pake, pendekatan kekeluargaan. Jadi, nasabah yang sudah terlanjur percaya sama kita sisa diyakinkan. 'pak, ibu ini namanya perbankan syariah mau berkembang oasti ada saja cobaannya, belum lagi banyak bank lain yang iri lihat perkembangannya yang terlalu cepat pesat, yang seharusnya 5 tahun dia capai di top 10 Global Islamic Bank hanya dengan 3 tahun dengan pencapaiannya.' Intinya kemarin Alhamdulillah tidak ada satupun nasabah yang hilang dananya, semuanya aman."[67]

Dari wawancara di atas, peneliti melanjutkan wawancara mengenai terkait hal yang sama dengan pak Ardiansya selaku *customer service*, sebagai berikut:

[67] Amiruddin, BOSM, wawancara oleh penulis di BSI Kcp Barru, 24 April 2024.

> "Kalo dari sisi *customer service* menangani keluhan nasabah, memang penting sistem jaringan karena betul-betul perbankan jasanya yang di butuhkan. Kapan sistemnya bermasalah orang-orang akan panik dan hilang kepercayaan, cuman disatu sisi kita sebagai pihak bank harus berpikir jangan merasa egois karena juga sangat dibutuhkan oleh masyarakat untuk menabung. Intinya kita kasih pengertian ke nasabah, jelaskan apa yang terjadi dan saling memberikan perhatian antara bank dan nasabah."[68]

Berdasarkan dari wawancara di atas dapat disimpulkan bahwa sebagaimana dua narasumber memberikan tanggapan dalam menangani keluhan para nasabah sesuai dengan jobdesk mereka masing-masing, artinya upaya pihak Bank Syariah Indonesia Kcp Barru betul-betul berusaha untuk menjaga kepercayaan nasabahnya dengan melakukan pendekatan, menjelaskan dan memberikan pemahaman terkait masalah yang terjadi agar nasabah merasaa tenang dan tidak panik di tengah isu yang beredar.

Wawancara berikutnya mengenai, pada saat terjadinya serangan yang di duga virus *ransomware* langkah apa yang di lakukan Bank Syariah Indonesia Kcp Barru dalam menjaga kepercayaan nasabah. Peneliti melakukan wawancara dengan pak Emir selaku *Branch Operation Service Manager* (BOSM), sebagai berikut:

> "Langkah yang di ambil Bank Syariah Indonesia Kcp Barru dengan itu tadi, kita meyakinkan nasabah baik lewat telepon, datangi rumahnya, kita pilah dulu mana nasaba besar mana nasabah besar mana nasabah proritas, mana nasabah haji, kita pilah dulu baru kita tarik kesimpulan. Ini yang kita prioritaskan dulu yang banyak dananya kita datangi satu-satu, jangan sampai nasabahnya yang datang komplai di bank lebih baik kita yang datangi duluan, minta maaf sampaikan yang sebenarnya kasih dia kesabara, kasih diapemahaman bahwa InsyaAllah akan secepatnya pulih, seperti itu yang kita lakukan. Alhamdulillah tidak ada yang komplain satu pun, tidak ada yang tarik dananya semuanya aman terkendali."[69]

[68] Ardiansya, *customer service*, wawancara oleh penulis di BSI Kcp Barru, 24 April 2024..
[69] Amiruddin, BOSM, wawancara oleh penulis di BSI Kcp Barru, 24 April 2024.

Dari wawancara di atas dengan pak Emir, peneliti melanjutkan wawancara terkait bagaimana solusi yang di berikan pihak bank BSI Kcp Barru kepada Julianti (nasabah) mengatakan bahwa :

> "Solusinya kemarin saya lihat ada pesan yang di kirimkan yang berisi permohonan maaf di *WhatsApp,* disitu juga menjelaskan bahwa adanya masalah gangguan jaringan yang terjadi dan pihak Bank juga memastikan bahwa dana maupun data nasabah juga aman. Selain itu, saya juga lihat status salah satu pegawai BSI disini, saya memang bukan nasabah prioritas tetapi tanggapan BSI juga membuat saya yakin masalah yang terjadi akan segera di atasi."[70]

Berdasarkan wawancara di atas dapat di simpulkan bahwa pihak Bank Syariah Indonesia Kcp Barru berhati-hati dalam mengambil langkah dalam menghadapi nasabah, apalagi di tengah situasi yang buruk ini banyaknya nasabah yang mengeluhkan terkait dana mereka terlebih pada nasabah besar maupun nasabah prioritas. Banyaknya kekhawatiran yang bakal terjadi tetapi pihak bank turun terlebih dahulu ke rumah-rumah nasabah untuk menyampaikan keadaan sebenarnya, bagaimana pihak bank juga menyampaikan permintaan maafnya ditengah keresahan para nasabah Bank Syariah Indonesia Kcp Barru.

Sebagaimana langkah awal Bank Syariah Indonesia Kcp Barru dalam menangani situasi tersebut yang sudah di bahas, terus bagaiamana dengan pihak bank dalam memulihkan layanan error yang diakibatkan oleh serangan. Wawancara terkait pertanyaan tersebut akan di jawab oleh pak Ardiansya selaku *customer service*, beliau menuturkan bahwa:

> "Terkait hal ini, kita sebagai pihak Bank Syariah Indonesia Kcp Barru tidak bisa berbuat apa-apa disini karena semua tergantung pusat, jadi kalo server pusat sudah bagus yah, berarti server di Bank Syariah Indonesia Kcp Barru juga bagus karena yang terjadi bukan hanya di Bank Syariah Indonesia Kcp Barru saja tetapi seluruh kantor cabang."[71]

[70] Julianti *nasabah*, wawancara oleh penulis di Lapakaka, 25 April 2024.
[71] Ardiansya, *customer service*, wawancara oleh penulis di BSI Kcp Barru, 24 April 2024.

Wawancara dilanjutkan oleh peneliti terkait dengan pertanyaan yang sama kepada pak Emir selaku *Branch Operation Service Manager* (BOSM), sebagai berikut:

> "Tentu saja, itu ada bagian ITnya Bnk Syariah Indonesia yang bekerja di pusat, sekarang ada penambahan IT yang melebihi biasanya yang 24 jam dengan pershif untuk perbaikan kecepatannya yang seharusnya pemindahan server itu 1 bulan menjadi 1 minggu oleh pihak Bank Syariah Indonesia."[72]

Berdasarkan wawancara keduanya dapat disimpulkan bahwa pemulihan layanan atau server yang error dilakukan oleh kantor pusat bagian khusus IT, semua kantor cabang tidak bisa melakukan banyak hal karena semua berpihak ke kantor pusat Bank Syariah Indonesia.

Peneliti menuturkan apakah setelah pemulihan server dilakukan, nasabah yang ada di Bank Syariah Indonesia Kcp Barru mengalami peningkatan, menurut pak Emir bahwa:

> "Nasabah makin meningkat, istilahnya ada sisi positif dan ada negatif lewat masalah yang terjadi, positifnya tambah yakin nasabah, banyak cara yang kita lakukan bagaimana nasabah tambah yakin sama bank BSI."[73]

Dari wawancara di atas, bahwa dari kejadian tersebut ada positifnya dan negatifnya bahkan setelah dilakukan pemulihan server nasabah yang ada di Bank Syariah Indonesia Kcp Barru malah mengalami peningkatan yang sangat signifikan. Banyaknya cara yang di lakukan pihak bank bagaimana menjaga kepercayaan nasabah hal ini di buktikan dengan peningkatan nasabah dalam menabung di Bank Syariah Indonesia Kcp Barru.

[72] Amiruddin, BOSM, wawancara oleh penulis di BSI Kcp Barru, 24 April 2024.
[73] Amiruddin, BOSM, wawancara oleh penulis di BSI Kcp Barru, 24 April 2024.

Selanjutnya peneliti melanjutkan wawancara dengan pak Ardiansya selaku *customer service* dengan pertanyaan, apakah ada kemungkinan serangan yang di duga virus *ransomware* bisa terjadi kembali, beliau menyampaikan bahwa:

> "InsyaAllah tidak karena sekarang fokusnya Bank Syariah Indonesia bagaimana agar hal ini tidak terjadi kembali, dikarenakan hal masalah ini kemarin ada direktur IT di kantor pusat Bank Syriah Indonesia yang diganti dari jabatannya karena saking fatalnya hal tersebut terjadi."[74]

Selain wawancara dilakukan di atas, peneliti juga melakukan wawancara denga pak Emir selaku *Branch Operation Service Manager* (BOSM) terkait hal yang sama, beliau menuturkan bahwa:

> "Kemungkinan InsyaAllah saya 98% itu tidak ada mi karena yang pertama dari sisi IT fokusnya dari Direksi memang itu fokus di IT selama 2 tahun terakhir ini, jadi semua dikesampingkan dari pembiayaannya, personalnya itu dikesampingkan jadi diutamakan untuk tahun 2023-2024 itu prioritas IT jadi semua keamanan itu diperketat bahkan akses ke komputer pegawai sendiri itu tidak sembarang diakses. Selama tidak ada persetujuan dari otoritas HP krarena ada pemberitahuan masuk, jangankan nasabah diperketat keamanannya, pegawai sendiri diperketat. Setiap minggu dilakukan pergantian *password* baik itu *password* ID maupun *password* servernya bank BSI. Sehingga akan sulit di *hack*, kalo serasa di *hack* kembali kecil kemungkinan terjadi."[75]

Berdasarkan dari hasil wawancara di atas dapat disimpulkan bahwa tanggapan keduanya menyatakan serangan virus *ransomware* kemungkinan tidak ada akan terjadi kembali dan menyerang Bank Syariah Indonesia, mereka memberikan alasan untuk memperkuat pernyataan keduanya. Hal ini Bank Syariah Indonesia telah mengalami perbaikan pada manajemen IT di kantor pusat sehingga kemungkinan kecil hal tersebut terjadi kembali. Kantor pusat

[74] Ardiansyah, *customer service*, wawancara oleh penulis di BSI Kcp Barru, 24 April 2024.
[75] Amiruddin, BOSM, wawancara oleh penulis di BSI Kcp Barru, 24 April 2024.

Bank Syariah Indonesia juga muli memperketat keamanan bank baik dari keamanan data nasabah maupun keamanan dari pegawai.

Wawancara selanjutnya dilakukan peneliti dengan pak Ardiansya selaku *customer service* dengan pertanyaan tindakan apa yang dilakukan Bank Syariah Indonesia kedepannya apabila hal serupa terjadi kembali, beliau menuturkan sebagai berikut:

> "Kalo bilang bagaimana usaha kedepannya, pasti berusaha tidak akan terjadi karena usaha Bank Syariah Indonesia pasti daari sisi IT nya diperbaiki, kecanggihannya diperbaiki, dan ditingkatkan keamanannya."[76]

Berdasarkan dari wawancara di atas dapat disimpulkan bahwa bagaimana upaya Bank Syariah Indonesia dalam menangani keluhan para nasabah, hal ini membuktikan bagaimana pihak bank sangat menjaga kepercayaan nasabahnya dengan melakukan pendekatan secara kekeluargaan yaitu meminta maaf terlebih dahulu, menjelaskan dan memberikan pemahaman terkait masalah yang sebenarnya sehingga nasabah merasa tenang akan dana maupun datanya. Langkah selanjutnya yang dilakukan pihak Bank Syariah Indonesia yaitu memulihkan layanan atau server yang error sebagai kantor pusat hal ini dilakukan perbaikan dalam manajemen IT dengan melakukan penambahan dan pemindahan server selama 1 minggu, apabila server atau layanan setelah diperbaiki maka kantor pusat Bank Syariah Indonesia menyampaikan ke kantor-kantor cabang bahwa layanan telah bisa dilakukan kembali.

Sebagaimana apabila hal serupa terjadi kembali Bank Syariah Indonesia sudah mengambil langkah untuk kedepannya dengan pergantian manajemen IT, melakukan pemeriksaan keamanan setiap minggu, keamanan data nasabah, pegawai pun mulai diperketat dan semankin ditingkatkan keamanannya sehingga makin sulit untuk diakses oleh pihak luar.

[76] Ardiansya, *customer service*, wawancara oleh penulis di BSI Kcp Barru, 24 April 2024

B. Pembahasan Hasil Penelitian

Dari keseluruhan hasil penelitian di atas, ada 3 fokus penelitian yang akan menjadi pembahasan di bawah ini, yaitu:

1. Bentuk serangan virus *ransomware* terhadap Bank Syariah Indonesia (BSI) di Kcp Barru

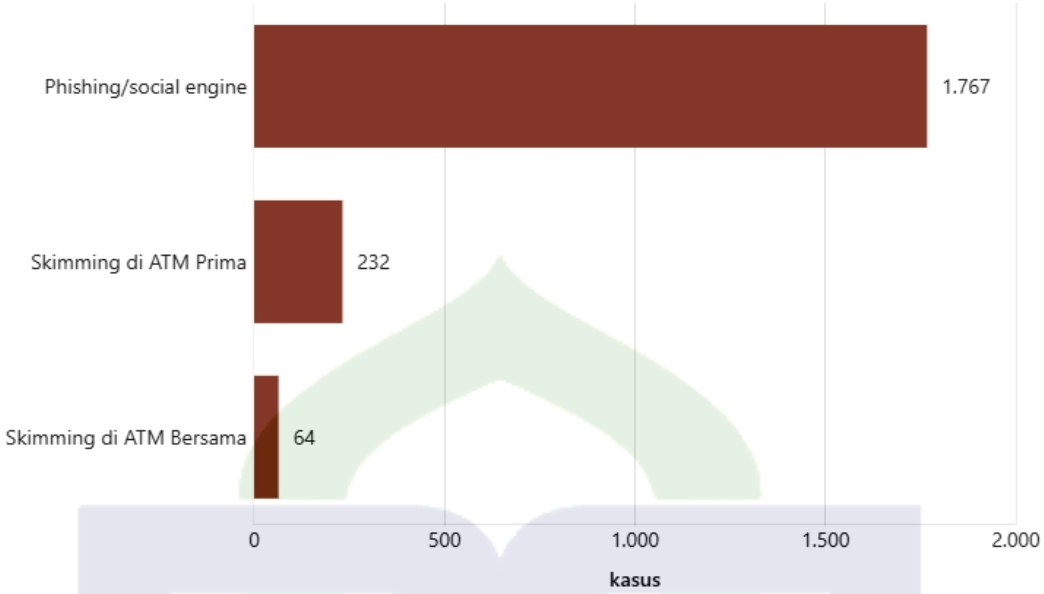
Virus *ransomware* adalah salah satu bentuk *malware* yang mengenkripsi data pada sistem komputer atau perangkat lainnya. Penyebarannya bisa melalui phising, lampiran berbahaya, email palsu, dan metode lainnya. Jenis perangkat lunak berbahaya ini membuat data tidak bisa diakses atau terenkripsi.

Dugaan serangan siber pada sistem aplikasi ini tampaknya merupakan kejadian pertama bagi Bank Syariah Indonesia (BSI). Heru Sutadi, Direktur Eksekutif ICT Institute, menyatakan bahwa ada kemungkinan aplikasi BSI mobile telah menjadi target serangan siber.

> "Kemungkinan besar, BSI terkena serangan siber yang memungkinkan sistemnya dikunci, atau tidak tertutup kemungkinan terkena *ransomware*."

Menurut laporan keberlanjutan Bank Syariah Indonesia (BSI), mereka mendeteksi lebih dari seribu insiden kejahatan siber pada tahun 2022. BSI mencatat 1.767 percobaan phising dan social engineering terhadap nasabahnya. Selain itu, terdapat 232 kasus kecurigaan skimming di jaringan ATM Prima dan 64 kasus di jaringan ATM Bersama, seperti yang tergambar dalam grafik di bawah ini:[77]

[77] Adi Ahdiat, "BSI Temukan Ribuan Ancaman Siber Pada 2022, Data Nasabah Diklaim Aman" (Jakarta, 2023).



Sumber : databoks.

Phising adalah jenis kejahatan siber yang melibatkan pengiriman tautan ke situs web palsu yang menyerupai situs asli kepada nasabah. Sementara itu, social engineering merupakan salah satu bentuk phishing, di mana pelaku berkomunikasi langsung dengan nasabah melalui telepon, SMS, atau saluran lainnya, untuk mengarahkan mereka ke situs tertentu dengan maksud mencuri data. Selain itu, skimming adalah tindakan mencuri informasi dari kartu ATM, yang termasuk dalam kategori kejahatan siber; metode ini biasanya dilakukan dengan memasang kamera tersembunyi pada mesin ATM untuk merekam nomor PIN nasabah.

Dalam insiden yang melibatkan Bank Syariah Indonesia, serangan yang diduga berasal dari virus *ransomware* mulai menyerang sistem TI di kantor pusat, mengakibatkan kerusakan pada server dan gangguan pada seluruh layanan bank. Serangan ini juga berdampak pada semua kantor cabang di Indonesia. Para pelaku meminta tebusan dalam bentuk mata uang digital untuk memulihkan data atau sistem yang terinfeksi. Situasi ini menimbulkan ketidaknyamanan dan

kecemasan bagi nasabah serta pemilik rekening, mengganggu operasional internal bank, dan berpotensi merusak kepercayaan masyarakat terhadap sistem perbankan. Kehilangan data berharga dan informasi keuangan bisa menyebabkan kerugian finansial yang signifikan bagi nasabah, serta merugikan reputasi bank. *Ransomware* sering dikaitkan dengan kelompok kejahatan yang mencari keuntungan melalui tindakan kriminal, menandakan bahwa *ransomware* dirancang sebagai alat pemerasan yang menargetkan perangkat elektronik.[78]

Seperti yang dijelaskan oleh peneliti dalam latar belakang, serangan virus *ransomware* telah mengakibatkan kehilangan data sebesar 1,5 TB, yang mencakup informasi sensitif. Hal ini berujung pada terjadinya kebocoran data di Bank Syariah Indonesia.[79] Berbeda dengan hasil penelitian yang di dapat melalui wawancara dari serangan virus *ransomware*, penyebab gangguan yang dialami Bank Syariah Indonesia di duga dari server IT yang bermasalah hingga merambat ke kantor cabang, pemulihan layanan atau server yang diperbaiki melalui penambahan server data selama 1 minggu, inilah yang menjadi adanya gangguan pada server IT Bank Syariah Indonesia. pihak Bank Syariah Indonesia Kcp Barru menyatakan bahwa serangan tersebut merupakan isu yang di buat-buat oleh sekelompok orang tertentu yang ingin merusak nama BSI, hal ini di buktikan melalui wawancara yang dilakukan dengan peneliti seperti yang tertera pada hasil penelitian. Pihak kantor pusat Bank Syariah Indonesia berani memberikan jaminan bahwa data-data semua nasabah aman dan tersimpan di server IT BSI, hal ini membuktikan bahwa tidak adanya kebocoran data yang terjadi seperti yang di isukan.

[78] Tajriyani, "Pertanggungjawaban Pidana Tindak Pidana Pemerasan Dengan Modus Operandi Penyebaran *Ransomware* Cryptolocker."

[79] Zahrani Fatni Hapsah and Muhammad Irwan Padli Nasution, "Analisis Tingkat Keamanan Data Perusahaan Yang Rentan Terhadap Serangan Cyber Dalam Sistem Informasi Manajemen," *Jurnal Manajemen Dan Akuntansi* 1, no. 2 (2023): 338–43.

Menurut manajemen Bank Syariah Indonesia dalam laporan keberlanjutannya yang dirilis pada tanggal 09 Mei 2023, beliau menuturkan bahwa :

> "Kami sampaikan bahwa Bank syariah Indonesia Tengah melakukan *maintenance* sistem sehingga tidak dapat diakses sementara waktu dan akan kembali ke kondisi normal secepatnya".

Manajemen Bank Syariah Indonesia (BSI) menyatakan bahwa masalah pada sistem IT menyebabkan seluruh layanan di semua kantor cabang tidak dapat diakses. Hal ini sejalan dengan hasil wawancara yang dilakukan peneliti di KCP Barru Bank Syariah Indonesia.

Penelitian ini tidak sejalan dengan riset yang dilakukan kelima penelitian terdahulu. Pertama, penelitian yang diselenggarakan oleh Kaira Milani Fitria yang menyatakan bahwa dalam perbedaannya yang hanya membahas berupa variasi solusi keamanan perusahaan untuk peningkatan sistem. [80] Kedua, penelitian yang dilakukan oleh Rendi Panca wijanarko,dkk menyatakan bahwa perbedaannya terletak pada hanya membahas untuk melakukan back up data yang dilakukan secara rutin sehingga mengurangi risiko terkena kembali serangan *ransomware.*[81] Ketiga, penelitian yang dilakukan oleh Mutmainnah mengungkapkan bahwa perbedaannya terletak pada tingkat kepercayaan nasabah, yang lebih memilih transaksi langsung dibandingkan dengan transaksi melalui internet banking. [82] Keempat, penelitian yang dilakukan oleh Sumarni yang menyatakan bahwa perbedaannya terletak pada pembahasan terkait nisbah bagi

[80] Kaira Milani Fitria, "Analisis Serangan *Malware* Dalam Perbankan Dan Perencanaan Solusi Keamanan," *Institut Informatika Dan Bisnis Darmajaya* 11, no. 3 (2023).

[81] Rendi Panca Wijanarko et al., "Analisis Dan Simulasi Serangan *Ransomware* Terhadap Database Bank Syariah Indonesia," *Universitas Pembanguan Nasioanal (UPN) Veteran Jakarta* 3, no. 1 (2023).

[82] Mutmainnah, "Tingkat Kepercayaan Nasabah BMI Cabang Parepare Dalam Menggunakan Internet Bangking Dan Transaksi Langsung," Institut Agama Islam Negeri, 2021.

hasi dan signifikaan terhadap kepercyaan nasabah.[83] Kelima, penelitian yang dilakukan oleh Anita Rahayu yang menyatakan bahwa perbedaannya terletak pada pembahasan dan peenelitian yang dilakukan terkait menangani komplain nasabah yang dilakukan sesuai standar dan implikasi strategi dalam menangani komplain yang berpegaruh pada tingkat kepuasan dan loyalitas nasabah.[84]

Berdasarkan dari hasil penelitian, fakta yang ditemukan bahwa Bank Syariah Kcp Barru membantah pernah terjadi serangan *hack* yang menimpa BSI yang menyebabkan banyak data nasabah bocor, sehingga hal tersebut membuat para nasabah Bank Syariah Indonesia banyak menarik dananya dan menyebabkan kerugian yang besar. Pihak Bank Syariah Indonesia Kcp Barru mengklaim tidak ada serangan melainkan kelalaian dari manajemen IT yang ada di kantor pusat BSI akibatnya membuat seluruh kantor cabang BSI mengalami error dari transaksi Automatic Teller Machine (ATM), error pada aplikasi BSI mobile banking, sehingga membuat para nasabah yang ingin melakukan transaksi secara online terhambat.

2. Dampak serangan virus *ransomware* terhadap kepercayaan nasabah Bank Syariah Indonesia (BSI) di Kcp Barru

Serangan virus *ransomware* memiliki dampak yang signifikan, seperti yang terlihat pada kasus Bank Syariah Indonesia (BSI) yang dikabarkan mengalami kebocoran data akibat serangan hacker. Sebanyak 15 juta data BSI termasuk informasi pengguna dan password untuk akses internal serta layanan bank dilaporkan bocor. Kebocoran data ini juga mencakup data karyawan, dokumen keuangan, dokumen legal, perjanjian kerahasiaan (NDA), dan lainnya. Data pelanggan yang terekspos meliputi nama, nomor telepon, alamat, saldo rekening, riwayat transaksi, tanggal pembukaan rekening, informasi pekerjaan,

[83] Sumarni, "Pengaruh Nisbah Bagi Hasil Terhadap Kepercayaan Nasabah DI BNI Syariah KCP Wonomulyo," Institut Agama Islam Negeri, 2021.

[84] Anita Rahayu, "Strategi Customer Service Dalam Manajemen Komplain Automatic Teller Machine (ATM) Pada Bank BTN Syariah Parepare," Institut Agama Islam Negeri, 2021.

dan sebagainya.[85] *Ransomware* kini merupakan ancaman besar di dunia digital. Serangan perangkat lunak berbahaya ini telah menimbulkan kerugian signifikan di berbagai sektor, terutama perbankan online. Kasus Bank Syariah Indonesia adalah contoh nyata betapa seriusnya dampak yang dihasilkan, yang tidak hanya mempengaruhi internal bank, tetapi juga eksternal bank. Selain itu, *ransomware* juga menyebabkan kerugian finansial dan kehilangan data yang signifikan.

Karena berbagai serangan yang terjadi, beberapa layanan perbankan BSI seperti mobile banking dan ATM mengalami masalah, yang membuat nasabah kesulitan dalam melakukan transaksi dan mengakses rekening mereka. Kondisi ini memicu kekhawatiran dan keluhan dari sejumlah nasabah mengenai gangguan yang mereka alami saat menggunakan layanan perbankan. Dampak dari serangan *Ransomware* ini pada Bank Syariah Indonesia adalah:

a. Gangguan Layanan Perbankan

Serangan tersebut menyebabkan terhentinya layanan perbankan di Bank Syariah Indonesia (BSI), termasuk mobile banking, ATM, dan sistem perbankan internal. Nasabah mengalami kesulitan dalam melakukan transaksi perbankan seperti biasa.

b. Kebocoran Data Sensitif

Serangan ini mengakibatkan data sensitif di Bank Syariah Indonesia (BSI) terpapar. Informasi nasabah seperti nomor rekening, data pribadi, dan informasi keuangan dapat jatuh ke tangan pihak yang tidak sah.

c. Gangguan Operasional

Operasional Bank Syariah Indonesia (BSI) terganggu akibat serangan tersebut. Tim IT harus fokus pada pemulihan sistem dan data yang terdampak, menyebabkan penundaan dalam layanan perbankan dan penanganan nasabah.

[85] Hapsah and Nasution, "Analisis Tingkat Keamanan Data Perusahaan Yang Rentan Terhadap Serangan Cyber Dalam Sistem Informasi Manajemen."

d. Kerugian Finansial

Serangan ini dapat menyebabkan kerugian finansial bagi Bank Syariah Indonesia (BSI). Selain biaya pemulihan dan perbaikan sistem, terdapat juga potensi pembayaran tebusan yang diminta oleh penyerang.

e. Kerugian Reputasi

Serangan terhadap Bank Syariah Indonesia (BSI) dapat merusak reputasi perusahaan. Nasabah dan masyarakat umum mungkin kehilangan kepercayaan terhadap keamanan data dan layanan perbankan BSI.

f. Ancaman Lanjutan

Keberhasilan serangan pada Bank Syariah Indonesia (BSI) dapat menarik perhatian serangan-serangan lain. Bank dan lembaga keuangan lainnya juga dapat menjadi target serupa, mengancam keamanan perbankan secara keseluruhan.

Dampak tersebut tidak hanya memengaruhi Bank Syariah Indonesia (BSI), tetapi juga berpengaruh pada nasabah serta masyarakat yang ingin memanfaatkan layanan perbankan. Hal ini bisa mengakibatkan penurunan reputasi BSI dibandingkan lembaga perbankan lainnya. Oleh karena itu, penting bagi BSI untuk meningkatkan keamanan siber, meningkatkan kesadaran di kalangan karyawan, dan menerapkan langkah-langkah pencegahan yang efektif untuk melindungi data nasabah serta memastikan kelangsungan layanan perbankan.

Adapun pada tinjauan teoritis pada macam-macam virus disebutkan bahwa ada beberapa dampak yang diberikan oleh masing-masing virus, seperti:

a. Malware

Perangkat lunak yang dibuat untuk merusak komputer, server, klien, atau jaringan. Ini dapat menyebabkan kerusakan pada sistem hard disk dan perangkat

lunak, mencuri data, serta merusak sistem informasi di komputer yang menjadi sasaran..

b. Phishing

Phishing bisa mengakibatkan pencurian informasi pribadi seperti data kartu kredit dan perbankan, serta kata sandi kredit. Ini terjadi ketika seseorang menyalahgunakan komunikasi online seperti email, telepon, atau pesan teks, menyamar sebagai lembaga resmi untuk memperoleh informasi sensitif secara tidak sah.

c. *Denial of Service* (DoS)

Denial of Service dapat mengakibatkan ketidaktersediaan sistem, membebani server, serta memperlambat atau bahkan menonaktifkan sistem untuk sementara waktu. Tinjauan teoritis dalam penelitian ini memberikan dasar yang kuat untuk memahami bagaimana virus dapat mengganggu sistem IT, baik pada komputer, sistem perusahaan, maupun sistem perbankan. Dalam konteks serangan *ransomware*, metode enkripsi digunakan untuk mengubah data menjadi format yang tidak dapat dibaca oleh perangkat. Hal ini membuat korban tidak dapat mengakses data mereka hingga informasi tersebut dipulihkan dari bentuk yang terenkripsi. *Ransomware* juga memiliki kemampuan untuk menyebar dan menginfeksi perangkat lain di sekitarnya.[86]

Penjelasan di atas, terkait dengan hasil penelitian yang di dapatkan bahwa Bank Syariah Indonesia mengalami dampak yang sangat besar terutama pada kantor-kantor cabang. Sebagaimana pada wawancara yang dilakukan peneliti pada Kantor Bank Syariah Indonesia Kcp Barru mengalami penurunan nasabah yang signifikan dikarenakan semua transaksi yang biasanya dilakukan baik secara online maupun offline mengalami gangguan sistem, akibatnya hal ini dapat mempengaruhi kepercayaan nasabah, larinya nasabah besar maupun nasabah prioritas, saingan dari pihak bank lain, seluruh jobdesk BSI mulai dari

[86] Russinovich, "Sony, Rootkits and Digital Rights Management Gone Too Far."

layanan gadai, customer service, teller tidak bisa beroperasi, mobile banking, bahkan transaksi melalui ATM juga mengalami gangguan bahkan pihak manajemen tidak bisa melakukan pengimputan data.

Ini sejalan dengan riset yang dilakukan oleh beberapa di bawah ini, Kaira Milani Fitriaa yang menunjukkan bahwa *ransomware*, sebuah jenis *malware* yang didesain untuk mengunci file korban dan meminta pembayaran agar kunci dekripsi diberikan.[87] Sama halnya dengan penelitian yang dilakukan oleh Rendi Panca Wijanarko, dkk. yang menyatakan bahwa dampak yang diakibatkan serangan *ransomware* terhadap infrastruktur database sebuah organisasi. [88] Namun, hasil penelitian Mutmainnah menunjukkan fokusnya tidak pada serangan *ransomware*.[89] Begitu pula dengan penelitian yang dilakukan oleh Sumarni yang juga tidak membahas terkait dampak serangan *ransomware* terhadap perbankan[90] Dan terakhir, penelitian yang dilakukan oleh Anita rahayu, yang hanya membahas manajemen komplain pada perbankan.[91]

Dari hasil penelitian yang didapatkan oleh peneliti bahwa pihak Bank Syariah Indonesia mengatakan adanya penurunan dan peningkatan pada jumlah nasabah setelah adanya masalah yang terjadi pada sistem IT Bank Syariah Indonesia. Dapat dilihat diagram batang di bawah menunjukkan perbandingan jumlah presentase nasabah pada kantor pusat Bank Syariah Indonesia dan Kantor cabang Bank Syariah Indonesia Kcp Barru.

---

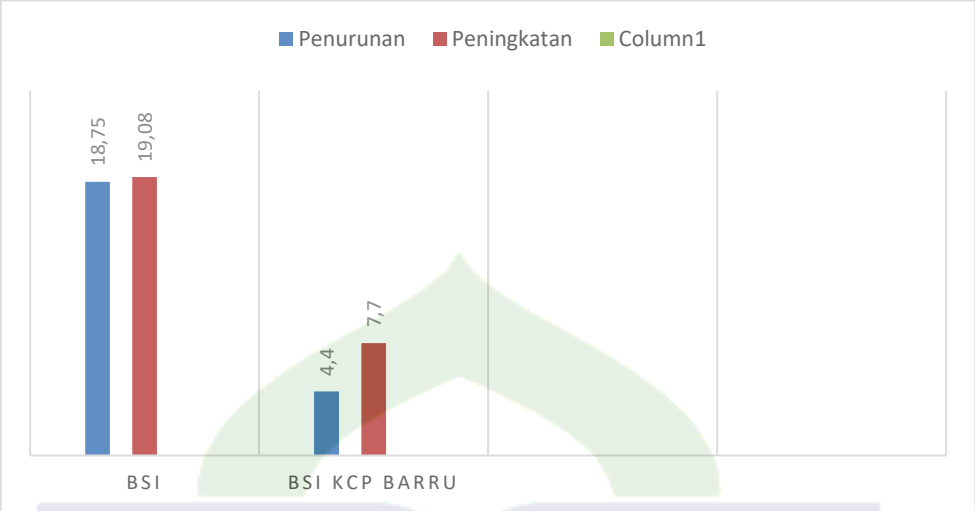
[87] Kaira Milani Fitria, "Analisis Serangan *Malware* Dalam Perbankan Dan Perencanaan Solusi Keamanan," *Institut Informatika Dan Bisnis Darmajaya* 11, no. 3 (2023).

[88] Rendi Panca Wijanarko et al., "Analisis Dan Simulasi Serangan *Ransomware* Terhadap Database Bank Syariah Indonesia," *Universitas Pembanguan Nasioanal (UPN) Veteran Jakarta* 3, no. 1 (2023).

[89] Mutmainnah, "Tingkat Kepercayaan Nasabah BMI Cabang Parepare Dalam Menggunakan Internet Bangking Dan Transaksi Langsung," Institut Agama Islam Negeri, 2021.

[90] Sumarni, "Pengaruh Nisbah Bagi Hasil Terhadap Kepercayaan Nasabah DI BNI Syariah KCP Wonomulyo," Institut Agama Islam Negeri, 2021.

[91] Anita Rahayu, "Strategi Customer Service Dalam Manajemen Komplain Automatic Teller Machine (ATM) Pada Bank BTN Syariah Parepare," Institut Agama Islam Negeri, 2021.



Dapat dilihat di atas bahwa Bank Syariah Indonesia mencatat pertumbuhan jumlah nasabah pada Q2 2023, salah satu direktur Teknologi Informasi Saladin D. Effendi mengatakan bahwa,

> "Pada Mei dan Juni 2023 jumlah nasabah BSI berjumlah 18,95 dan 19,08 juta nasabah. Dengan kata lain, jumlah nasabah BSI terus mengalami peningkatan setiap bulannya".[92]

Sedangkan jumlah nasabah Bank Syariah Indonesia Kcp Barru mengalami penurunan nasabah pada bulan Mei diakibatkan adanya masalah pada sistem IT tetapi, peningkatan jumlah nasabah secara signifikan kembali terjadi pada bulan berikutnya yaitu 7,7. Hal ini di katakan langsung oleh *Branch Operation Service Manager* (BOSM) bahwa:

> "Peningkatan jumlah nasabah terus meningkat perharinya dari ada 6 sampai 7 nasabah yang melakukan pembukaan rekening kini meningkat menjadi 15 nasabah, bisa dikatakan kalo di total pada bulan Mei kemarin sekitar 35 nasabah di cabang barru yang bertambah. Apabila di kali 22 hari kerja ada 7,7 nasabah yang bertambah setiap bulannya".[93]

[92] Putri Hanifa, "BSI Catat Pertumbuhan Jumlah Nasabah 10,9 Persen per September 2023," Antara Kantor Berita Indonesia, 2023.

[93] Amiruddin, BOSM, wawancara oleh penulis di BSI Kcp Barru, 29 Juli 2024.

Dari berbagai penjabaran di atas dapat di tarik kesimpulan yaitu, bagaimana dampak yang di berikan cukup berpengaruh pada kepercayaan nasabah ini menunjukkan bahwa dari masalah yang terjadi dapat memberikan dampak negatif yang cukup besar pada Bank Syariah Indonesia, mulai dari larinya semua nasabah sehingga terjadinya penurunan, transaksi yang tidak bisa dilakukan baik secara maupun offline, hingga berdampak pada reputasi bank, dari hasil wawancara sebelumnya juga dikatakan setelah terjadinya masalah ini dapat memberikan solusi bagi pihak Bank Syariah bagaimana menghadapi dan mengatasi masalah yang terjadi bisa dikatakan hal ini dapat memberikan dampak positif atau Pelajaran yang bisa diambil bagi pihak bank.

3. Upaya Bank Syariah Indonesia (BSI) di Kcp Barru dalam memulihkan kepercayaan nasabah setelah terjadinya serangan virus *ransomware*

Terkait dampak serangan virus *ransomware* pada Bank Syariah Indonesia Kcp Barru diperlukan adanya upaya atau tindakan yang serius dalam mengatasi masalah tersebut dan diperlukan adanya langkah pencegahan kedepannya agar hal tersebut tidak terjadi kembali. Perlindungan data sistem dari serangan yang merusak dan merugikan harus menjadi fokus utama bagi lembaga keuangan dan organisasi lainnya dalam era digital ini. Menurut Budi Hartono, penting untuk melakukan langkah antisipatif guna mencegah serangan seperti *ransomware* yang dapat merusak sistem dengan cara *hacking*. Untuk itu, beberapa langkah *preventif* dapat diimplementasikan:

a. Lakukan pencadangan data secara rutin : Cadangkan data penting ke lokasi aman seperti penyimpanan eksternal atau *cloud* secara teratur. Pastikan pencadangan otomatis dan terverifikasi.

b. Perbarui perangkat lunak dan sistem operasi : Selalu perbarui sistem operasi, aplikasi, dan perangkat keras dengan versi terbaru untuk menutup kerentanan dan mencegah serangan *ransomware*.

c. Gunakan solusi keamanan yang handal : Instal perangkat lunak keamanan terpercaya seperti *antivirus, antispyware*, dan *firewall*.

d. Pilih kata sandi yang kuat : Gunakan kata sandi kompleks dengan kombinasi huruf, angka, dan simbol. Manfaatkan manajer kata sandi untuk mengelola sandi yang berbeda untuk setiap akun.

e. Batasi hak akses : Berikan hak akses yang sesuai untuk pengguna dan kelompok, serta batasi akses administrator hanya kepada yang memerlukan untuk mengurangi risiko penyebaran *ransomware*.[94]

Bank BSI akan terus meningkatkan digitalisasi dan keamanan sistem, terutama dalam melindungi informasi dan dana nasabah. Langkah *preventif* juga dilakukan untuk memperkuat keamanan teknologi informasi terhadap potensi gangguan data, dengan meningkatkan kemampuan dan ketahanan sistem. Secara bersamaan, Bank Syariah Indonesia juga melakukan penyelidikan internal dan terus berkoordinasi dengan Badan Siber dan Sandi Negara (BSSN), Otoritas Jasa Keuangan (OJK), Bank Indonesia (BI), serta instansi lainnya.[95] Bank Syariah Indonesia (BSI) menyatakan bahwa mayoritas nasabahnya merasa aman dan terlindungi saat menggunakan layanan mereka. Meskipun demikian, perusahaan tetap berkomitmen untuk terus meningkatkan privasi dan keamanan bagi nasabah.[96]

Penjelasan diatas, terkait upaya dalam mencegah serangan *ransomware* hal ini sesuai dengan hasil penelitian yang di temukan bahwa upaya Bank Syariah Indonesia dalam pencegahan *hacking* yang pertama, menjaga keamanan sistem IT dengan melakukan pergantian manajemen yang kedua, menambah kapasitas server data yang ketiga, akses ke semua perangkat komputer pegawai

[94] Budi Hartono, "*Ransomware*: Memahami Ancaman Keamanan Digital," *Bincang Sains Dan Teknologi* 2, no. 02 (2023): 55–62, https://doi.org/10.56741/bst.v2i02.353.

[95] Achmad Ghifari Firdaus, "Layanan Sempat Eror, OJK: Berbagai Upaya BSI Akan Kembalikan Kepercayaan Nasabah" (Jakarta, 2023).

[96] Lavinda, "Aplikasi Kena Serangan Siber, Ini Upaya BSI Lindungi Data Nasabah" (Jakarta, 2023).

mulai di perketat dengan dilakukannya pengecekkan dan pergantian *password* sehingga akan sulit untuk di *hack* dan keempat, seluruh keamanan data baik data nasabah maupun pegawai mulai diperketat.

Berdasarkan dari hasil penelitian, dalam menangani keluhan nasabah terhadap layanan error pada BSI mobile ataupun ATM yaitu dengan melakukan pendekatan, mnjelaskan dan memberikan pemahaman kepada nasabah terkait masalah yang terjadi, menyampaikan permintaan maaf dan mendatangi nasabah sehingga nasabah juga yakin dengan pihak bank.

Penelitian ini sejalan dengan temuan Kaira Milani Fitria, yang menekankan bahwa menjaga keamanan merupakan fondasi penting dalam menghadapi ancaman *malware* di *mobile banking*. Diperlukan penerapan teknologi baru serta langkah-langkah keamanan proaktif yang terus dilakukan untuk melindungi integritas sistem perbankan.[97] Penelitian oleh Rendi Panca Wijanarko dan tim menunjukkan bahwa salah satu langkah yang diambil adalah melakukan pencadangan data secara berkala dan menyimpannya terpisah dari perangkat utama yang digunakan.[98] Namun, tidak sejalan dengan penelitian yang dilakukan oleh Mutmainnah, yang tidak membahas terkait serangan *ransomware*.[99] Begitu pula dengan penelitian yang dilakukan oleh Sumarni yang juga tidak membahas terkait dampak serangan *ransomware* terhadap perbankan.[100] Dan terakhir, penelitian yang dilakukan oleh Anita rahayu, yang hanya membahas manajemen komplain pada perbankan.[101]

---

[97] Kaira Milani Fitria, "Analisis Serangan *Malware* Dalam Perbankan Dan Perencanaan Solusi Keamanan," *Institut Informatika Dan Bisnis Darmajaya* 11, no. 3 (2023).

[98] Rendi Panca Wijanarko et al., "Analisis Dan Simulasi Serangan *Ransomware* Terhadap Database Bank Syariah Indonesia," *Universitas Pembanguan Nasioanal (UPN) Veteran Jakarta* 3, no. 1 (2023).

[99] Mutmainnah, "Tingkat Kepercayaan Nasabah BMI Cabang Parepare Dalam Menggunakan Internet Bangking Dan Transaksi Langsung," Institut Agama Islam Negeri, 2021.

[100] Sumarni, "Pengaruh Nisbah Bagi Hasil Terhadap Kepercayaan Nasabah DI BNI Syariah KCP Wonomulyo," Institut Agama Islam Negeri, 2021.

[101] Anita Rahayu, "Strategi Customer Service Dalam Manajemen Komplain Automatic Teller Machine (ATM) Pada Bank BTN Syariah Parepare," Institut Agama Islam Negeri, 2021.

Dari berbagai penjabaran di atas upaya Bank Syariah Indonesia Kcp Barru dalam memulihkan kepercayaan nasabah dapat di simpulkan bahwa pihak bank menunjukkan bagaimana mereka memberikan pengertian, menjelaskan terkait masalah transaksi yang tidak bisa di lakukan, mereka meyakinkan dana nasabah maupun data nasabah aman dan tidak sesuai dengan yang di isukan, pihak bank berani bertanggung jawab apabila hal tersebut terjadi.

Menurut *Corporate Secretary* BSI Gunawan A Hartoyo menyatakan dalam wawancara liputan 6 bahwa "Data dan dana nasabah aman, serta aman dalam bertransaksi. Kami berharap nasabah tetap tenang dalam bertransaksi dan kami juga memastikan bekerjasama dengan otoritas terkait dengan isu kebocoran data."[102]

Hasil penelitian ini dikaitkan dengan penelitian terdahulu bahwa relevansi hasil penelitian dengan penelitian-penelitian sebelumnya yang telah disebutkan terletak pada kesamaan topik yang di teliti, yaitu virus *ransomware* dan kepercayaan nasabah, namun dengan fokus yang berbeda. Hasil penelitian yang membahas dampak hoax terkait isu serangan virus *ransomware* terhadap kepercayan nasabah dalam penyimpanan dana di Bank Syaariah Indonesia (BSI) Kcp Barru, memiliki kesamaan dengan penelitian lain dalam hal mendalami kepercayaan nasabah.

Meskipun fokus penelitian berbeda, namun ada beberapa kesamaan yang dapat di identifikasi. Salah satunya adalah bagaimana dampak dari suatu masalah cukup mempengaruhi kepercayaan nasabah. Temuan ini mencerminkan adanya perbedaan yang cukup menonjol dalam dampak yang diberikan hoax terkait isu virus *ransomware*.

Secara umum, temuan dari penelitian ini memberikan sumbangan signifikan terhadap pemahaman tentang serangan virus *ransomware* yang

[102] Natasha Khairunisa Amani, "Fakta-Fakta BSI Kena Serangan Siber Kelompok *Ransomware* Lockbit" (Jakarta, 2023).

mempengaruhi kepercayaan nasabah di Bank Syariah Indonesia Kcp Barru. Di samping itu, penelitian ini juga membandingkan dengan studi-studi sebelumnya. Selain itu, melalui perbandingan dengan penelitian-penelitian sebelumnya, dapat dilihat kesamaan dan perbedaan pada penelitian ini, sehingga dapat memberikan informasi yang berharga bagi pengembangan pengetahuan dan pemahaman tentang perbandingan upaya Bank Syariah Indonesia Kcp Barru dalam memulihkan layanan dan kepercayaan nasabah dalam berbagai situasi daan lingkungan yang berbeda.

BAB V

PENUTUP

A. Simpulan

Berdasarkan hasil penelitian yang telah dilakukan oleh peneliti mengenai Dampak Hoax Terkait Isu Serangan Virus *Ransomware* Terhadap Kepercayaan Nasabah Di BSI Kcp Barru. Maka dapat ditarik simpulan sebagai berikut:

1. Bentuk serangan yang diduga virus *ransomware* terhadap Bank Syariah Indonesia (BSI) di Kcp Barru, Virus *ransomware* merupakan salah satu virus *malware* yang berupa perangkat lunak berbahaya yang di duga menyerang sistem IT Bank Syariah Indonesia sehingga berdampak pada semua kantor cabang. Menurut pegawai bank yang telah banyak memberikan informasi mengenai bentuk serangan yang menyerang sistem IT Bank Syariah Indonesia, "kalaupun ada isu yang mnyatakan bahwa serangan *ransomware* yang menyerang BSI, itu hanya sebuah isu yang di beritakan untuk merusak nama baik BSI. Penyebabnya bukan karena serangan melainkan proses penambahan server IT yang membuat error jaringan di semua sistem BSI." Ini membuktikan bahwa bentuk serangan yang di duga virus rasomware merupakan isu yang beredar tidaklah benar, melainkan adanya masalah internal yang terjadi yaitu peenambahan server data IT di Bank Syariah Indonesia.
2. Dampak serangan virus *ransomware* terhadap kepercayaan nasabah Bank Syariah Indonesia (BSI) di Kcp Barru, sebagaimana yang di dapat dari hasil penelitian, kantor cabang satu ini banyak mengalami dampak yang terjadi mulai dari penurunan nasabah, semua transaksi baik secara online maupun offline tidak bisa beroperasi dengan baik sehingga berdampak pada dana nasabah, bahkan seluruh jobdesk Bank Syariah Indonesia Kcp Barru tidak bisa melakukan pengimputan.

3. Upaya Bank Syariah Indonesia (BSI) di Kcp Barru dalam memulihkan kepercayaan nasabah setelah terjadinya serangan virus *ransomware*, diperlukan tindakan yang dilakukan oleh kantor pusat Bank Syariah Indonesia dengan mengambil kangkah awal untuk menjaga keamanan digital menjadi prioritas utama, melindungi data sistem nasabah maupun data rahasi bank, upaya selanjutnya yang dilakukan oleh kantor pusat yaitu mengganti manajemen IT yang menyebabkan masalah yang teerjadi, akses ke semua perangkat komputer pegawai mulai ddi perkeetat sehinggan akan sulit untuk terjadi masalah yang serupa. Bank syariah Indonesia Kcp Barru sendiri memberikan tanggapan bahwa upaya yang mereka lakukan adalah dengan meyakinkan kembali nasabah bahwa semua dana nasabah aman dan tidak terganggu, selain itu dengan melakukan pendekatan secara kekeluargaan.

B. Saran

1. Bank Syariah Indonesia cabang Barru diminta untuk meningkatkan kesadaran terhadap keamanan dan perlindungan data, serta lebih waspada terhadap potensi kejahatan yang dapat merugikan nasabah dan bank itu sendiri. Peningkatan kepercayaan nasabah terhadap sistem keamanan IT harus menjadi perhatian utama demi menjaga keamanan dan kenyamanan bersama.
2. Perpustakaan diharapkan dapat menjadi sumber referensi yang berguna untuk mendukung penelitian lebih lanjut mengenai dampak dari serangan virus *ransomware* terhadap kepercayaan nasabah di Bank Syariah Indonesia cabang Barru.

DAFTAR PUSTAKA

Ahdiat, Adi. “BSI Temukan Ribuan Ancaman Siber Pada 2022, Data Nasabah Diklaim Aman.” Jakarta, 2023.

Amani, Natasha Khairunisa. “Fakta-Fakta BSI Kena Serangan Siber Kelompok *Ransomware* Lockbit.” Jakarta, 2023.

Andesra, Yuli. “Peran Kualitas Pelayanan Dalam Mebangun Kepercayaan Dan Loyalitas Nasabah Bank Syariah Mandiri Cabang Simpang Empat.” *Jurnal Apresiasi Ekonomi* 4, no. 2 (2019): 138–50. https://doi.org/10.31846/jae.v4i2.157.

Arif, M.Nur Rianto Al. *Dasar-Dasar Pemasaran Bank*. Jakarta: CV Rajawali, 1994.

Astarina, Ivalaina, and Angga Hapsila. *Manajemen Perbankan*. Edited by Puspa Dewi and Syafrizal. *Deepublish (Grup Penerbit CV Budi Utama)*. 1st ed. Yogyakarta: Deepublish (Grup Penerbit CV Budi Utama), 2015.

Bank, Shinhan. “PENGERTIAN INTERNET BANKING.” Shinhan Bank, 2017. https://www.shinhan.co.id/article-listings/read/pengertian-internet-banking.

Biotika. “Manfaat Dan Contoh Penerapan Teknologi Informasi Dalam Dunia Perbankan.” Biotika, 2021. https://botika.online/about-us/index.php.

Budi Setiawan, Mulyo, and Ukudi Ukudi. “Pengaruh Kualitas Layanan, Kepercayaan Dan Komitmen Terhadap Loyalitas Nasabah (Studi Pada Pd. Bpr Bank Pasar Kendal).” *Jurnal Bisnis Dan Ekonomi (JBE), September 2007, Hal. 215-227 Vol.14, No.2* 14, no. 2 (2007): 215–27.

Budiono, I Nyoman. *Manajemen Pemasaran Bank Syariah*. Edited by Asriadi Arifin. Parepare: IAIN Parepare Nusantara Press, 2022.

Djahir, Yulia, and Dewi Pratita. *Sistem Informasi Manajemen*. Yogyakarta: Deepublish (Grup Penerbit CV Budi Utama), 2014.

Farid, Achmad. “14 Kasus Cyber Crime Di Indonesia Yang Menggemparkan Warganet.” Exabytes, 2022. https://www.exabytes.co.id/blog/category/cyber-security/.

Fasochah, and Harnoto. “Analisis Pengaruh Kepercayaan Dan Kualitas Layanan Terhadap Loyalitas Pelanggan Dengan Kepuasan Konsumen Sebagai Variabel Mediasi (Studi Pada RS Darul Istiqomah Kaliwungu Kendal) Hartono.” *Jurnal Ekonomi Manajemen Akuntansi* 20, no. 34 (2013): 1–14.

Faulina, Aulia Reta. “Apa Itu *Ransomware*, Jenis, Penyebab, Dan Cara Mencegahnya.” Sekawan Media, 2023. https://www.sekawanmedia.co.id/blog/apa-itu-*ransomware*/#:~:text=Penyebab

Ransomware 1 1. Phishing Penyebarannya sering kali,Tidak Terlindungi ... 5 5. Pembayaran *Ransomware*.

Firdaus, Achmad Ghifari. "Layanan Sempat Eror, OJK: Berbagai Upaya BSI Akan Kembalikan Kepercayaan Nasabah." Jakarta, 2023.

Fitria, Kaira Milani. "Analisis Serangan *Malware* Dalam Perbankan Dan Perencanaan Solusi Keamanan." *Institut Informatika Dan Bisnis Darmajaya* 11, no. 3 (2023). https://doi.org/10.23960/jitet.v11i3.3312.

Fitriani, Yuni, and Roida Pakpahan. "Analisa Penyalahgunaan Media Sosial Untuk Penyebaran Cybercrime Di Dunia Maya Atau Cyberspace." *Cakrawala : Jurnal Humaniora* 20, no. 1 (2020): 2579–3314.

Hanifa, Putri. "BSI Catat Pertumbuhan Jumlah Nasabah 10,9 Persen per September 2023." Antara Kantor Berita Indonesia, 2023.

Hapsah, Zahrani Fatni, and Muhammad Irwan Padli Nasution. "Analisis Tingkat Keamanan Data Perusahaan Yang Rentan Terhadap Serangan Cyber Dalam Sistem Informasi Manajemen." *Jurnal Manajemen Dan Akuntansi* 1, no. 2 (2023): 338–43.

Hardiansyah, Zulfikar. "Kasus Serangan *Ransomware* Di Indonesia, BI Pernah Jadi Sasaran." Accessed July 27, 2024. https://tekno.kompas.com/read/2023/05/16/14300037/kasus-serangan-*ransomware*-di-indonesia-bi-pernah-jadi-sasaran?page=all#page2.

Hariyati, Sinta. "Persepsi Masyarakat Terhadap Pembangunan Jembatan Mahkota Ii Di Kota Samarinda." *Journal Ilmu Pemerintahan* 3, no. 2 (2008): 585–96.

Hartono, Budi. "*Ransomware*: Memahami Ancaman Keamanan Digital." *Bincang Sains Dan Teknologi* 2, no. 02 (2023): 55–62. https://doi.org/10.56741/bst.v2i02.353.

Informasi, Kanal. "Pengertian Siber (Cyber)." lentera kecil grup, 2023. https://www.kanalinfo.web.id/pengertian-siber-cyber#:~:text=Sedangkan secara etimologi cybernetics berasal dari bahasa Yunani,kybernēt" yang berarti "terampil dalam mengatur atau memerintah."

Kasmir. *Pemasaran Bank*. Revisi. Jakarta: Kencana, 2004.

Kusuma, DEwi Intan. "Pengaruh Kepercayaan Terhadap Loyalitas Konsumen Pada Bedak My Baby (Studi Pada Siswi SMKN2 Kediri Kelas XI)." *Skripsi Iain Kediri*, 2021, 21–33.

Lavinda. "Aplikasi Kena Serangan Siber, Ini Upaya BSI Lindungi Data Nasabah." Jakarta, 2023.

Muchdi, Baderi Imam. "'Definisi Keamanan Siber (Cyber Security).'"

Kompasiana.com, 2020. https://www.kompasiana.com/baderi/5f250f52097f360b3c6f6222/definisi-keamanan-siber-cyber-security?page=2&page_images=1.

Mutmainnah. "Tingkat Kepercayaan Nasabah BMI Cabang Parepare Dalam Menggunakan INternet Bangking Dan Transaksi Langsung." *Skripsi Iain Parepare*, 2021.

Napizahni, Mike. "Apa Itu *Ransomware*? Pengertian, Jenis, Dan Cara Mengatasinya." PT DEWAWEB, 2022. https://www.dewaweb.com/blog/apa-itu-*ransomware*/#Apa_Itu_*Ransomware.*

Pintarnya. "User," 2023.

Presiden Republik Indonesia. "Undang-Undang Republik Indonesia Nomor 10 Tahun 1998 Tentang Perubahan Atas Undang-Undang Nomor 7 Tahun 1992 Tentang Perbankan." *Lembaran Negara Republik Indonesia*, 1998, pasal 1 ayat 3.

Publik, Administrasi. "Manajemen Bank : Pengertian, Tujuan, Fungsi, Struktur, Dan Unsur - Unsur Dalam Manajemen Bank," 2023.

Rahayu, Anita. "Strategi Customer Service Dalam Manajemen Komplain Automatic Teller Machine (ATM) Pada Bank BTN Syariah Parepare." *Skripsi Iain Parepare*, 2021.

RI, Kementerian Agama. "Al-Qur'an Dam Terjemahannya, Q.S. Al-Baqarah, 205," 2019.

———. "Qura'an Kemenag, Al-Qur'an Dan Terjemahahnnya." Q.S. Ali-imran, n.d. https://lajnah.kemenag.go.id.

Ricardo, Edward. "BSI Diserang *Ransomware*, Nasib Uang Nasabah Gimana?" Redaksi, CNBC Indonesia, 2023. https://www.cnbcindonesia.com/tech/20230510174928-37-436279/bsi-diserang-*ransomware*-nasib-uang-nasabah-gimana.

Rivai, Veithzal, Andria Permata Veithzal, and Ferry N Indroes. *Bank and Financial Institution Management*. Jakarta: PT RajaGrafindo Persada, Jakarta, 2007.

Robbins, Stephen P, and Timothy A Judge. *Perilaku Organisasi*. Jilid 2. Jakarta: Salemba Empat, 2011.

Russinovich, Mark. "Sony, Rootkits and Digital Rights Management Gone Too Far." Mark's Blog, 2005. https://webcitation.org/686ime0m5?url=http://blogs.technet.com/b/markrussinovich/archive/2005/10/31/sony-rootkits-and-digital-rights-management-gone-too-far.aspx.

Sajjan, Rajani S, and Vijay R Ghorpade. "*Ransomware* Attacks: Radical Menace for

Cloud Computing." *Proceedings of the 2017 International Conference on Wireless Communications, Signal Processing and Networking, WiSPNET 2017* 2018-Janua, no. March 2017 (2017): 1640–46. https://doi.org/10.1109/WiSPNET.2017.8300039.

Sari, Lily Nur Indah. "Dampak Pembiayaan BNI Syariah Kcp Wonomulyo Terhadap Peningkatan UMKM." *Institut Agama Islam Negeri Parepare* 10, no. 2 (2021): 10. http://www.theseus.fi/handle/10024/341553%0Ahttps://jptam.org/index.php/jptam/article/view/1958%0Ahttp://ejurnal.undana.ac.id/index.php/glory/article/view/4816%0Ahttps://dspace.uii.ac.id/bitstream/handle/123456789/23790/17211077 Tarita Syavira Alicia.pdf?

Soekanto, Soerjono. *Sosiologi Suatu Pengantar*. Revisi. Jakarta: Rajawali Pers, 2017.

Sudirman, I Wayan. *Manajemen Perbankan*. Edited by Riefmanto. 1st ed. Jakarta: Kencana, Prenada Media Group, 2013.

Suharno, and Retnoningsih. *Kamus Besar Bahasa Indonesia*. Semarang: Widya Karya, 2003.

Sumarni. "Pengaruh Nisbah Bagi Hasil Terhadap Kepercayaan Nasabah DI BNI Syariah KCP Wonomulyo." *Skripsi Iain Parepare*, 2021.

Tajriyani, Nur Syamsi. "Pertanggungjawaban Pidana Tindak Pidana Pemerasan Dengan Modus Operandi Penyebaran *Ransomware* Cryptolocker." *Jurist-Diction* 4, no. 2 (2021): 685. https://doi.org/10.20473/jd.v4i2.25785.

Tasmara, K.H. Toto. *Membudayakan Etos Kerja Islam*. Jakarta: Gema Insani, 2002.

Tjiptono, Fandy. *Pemasaran Jasa: Prinsip, Penerapan Dan Penelitian*. Yogyakarta: Andi Offset, 2014.

Ubaidah, Ahmad Nur. "Tipe Virus *Ransomware* Dan Solusi Terbaik Mengatasinya." Logique, 2021. https://www.logique.co.id/blog/2021/01/07/tipe-virus-*ransomware*/#:~:text=Terdapat ciri-ciri perangkat Anda telah terinfeksi oleh virus,yang sebelumnya digunakan pada perangkat Anda. More items.

Usman, Nuramaliah Fakhriani. "Prefrensi Nasabah Terhadap Penggunaan Layanan Internet Bangking Di Bank Mandiri Parepare." *Skripsi*, 2020.

Wahidin, Gratiyo Wahyu, Syaifuddin Syaifuddin, and Zamah Sari. "Analisis *Ransomware* Wannacry Menggunakan Aplikasi Cuckoo Sandbox." *Jurnal Repositor* 4, no. 1 (2022): 83–94. https://doi.org/10.22219/repositor.v4i1.1373.

Widodo, Singgih Arif, Alimuddin Yasin, and Khurotul Aeni. "KEAMANAN JARINGANFIREWALL DAN IDS." Yogyakarta, 2015.

Wijanarko, Rendi Panca, Moch Rezeki Setiawan, Siti Mukaromah, and Abdul Rezha

Efrat Najaf. "Analisis Dan Simulasi Serangan *Ransomware* Terhadap Database Bank Syariah Indonesia." *Universitas Pembanguan Nasioanal (UPN) Veteran Jakarta* 3, no. 1 (2023): 106–15. https://doi.org/10.33005/sitasi.v3i1.436.

Wijaya, Andy Nova. "Pengertian Dan Fungsi Firewall," 2014.

Wikipedia bahasa Indonesia, ensiklopedia bebas. "*Malware*," 2023. https://id.wikipedia.org/wiki/*Malware*.

Zaki. "Pengertian Manajemen Perbankan Adalah: Tahapan, Resiko," 2023.

Zubair, Muhammad Kamal. *Penulisan Karya Ilmiah Berbasis Teknologi Informasi*. Terbaryu. Parepare, 2021.

LAMPIRAN

	KEMENTRIAN AGAMA REPUBLIK INDONESIA INSTITUT AGAMA ISLAM NEGERI PAREPARE FAKULTAS EKONOMI DAN BISNIS ISLAM **Jl. Amal Bakti No. 8 Soreang 91131 Telp. (0421) 21307**
	VALIDASI INSTRUMEN PENELITIAN

NAMA MAHASISWA	:	NUR AZIZAH
NIM	:	2020203861206013
FAKULTAS	:	EKONOMI DAN BISNIS ISLAM
PRODI	:	PERBANKAN SYARIAH
JUDUL	:	DAMPAK SERANGAN VIRUS RANSOMWARE TERHADAP TINGKAT KEPERCAYAAN NASABAH DALAM PENYIMPANAN DANA DI BSI KCP BARRU

Pedoman Wawancara

1. Apakah serangan virus *ransomware* dapat mempengaruhi kepercayaan nasabah?
2. Apakah terjadi peningkatan atau penurunan nasabah dalam menyimpan dana di BSI kcp Barru?
3. Apa yang menjadi kendala dalam menyimpan dana di BSI Kcp barru saat terjadinya serangan virus *ransomware*?
4. Apakah ada pengaruh serangan yang timbul virus terhadap jobdesk di BSI Kcp Barru?
5. Bagaimana dampak yang di sebabkan serangan virus *ransomware* di BSI Kcp Barru?

6. Pada saat terjadinya serangan virus *ransomware* langkah apa yang dilakukan BSI Kcp Barru dalam menjaga kepercayaan nasabah?
7. Bagaimana BSI kcp Barru memulihkan layanan yang error yang diakibatkan oleh virus *ransomware*?
8. Apakah ada kemungkinan serangan virus ini bisa terjadi Kembali? Jika tidak, apa sebabnya anda berargumen mengatakan tidak?
9. Bagaimana strategi BSI kcp barru dalam menangani keluhan nasabah terhadap layanan yang error?
10. Tindakan apa yang dilakukan BSI Kcp Barru kedepannya apabila hal serupa mungkin terjadi kembali?

Parepare, 22 Februari 2024

Mengetahui,

Pembimbing Utama	Pembimbing Pendamping
Dr. And Bahri S. M.E., M.Fil.I.	Dr. Musmulyadi, S.HI., M.M.
NIP : 197811012009121003	NIP : 199103072019031009

KEMENTERIAN AGAMA REPUBLIK INDONESIA
INSTITUT AGAMA ISLAM NEGERI PAREPARE
FAKULTAS EKONOMI DAN BISNIS
Jalan Amal Bakti No. 8 Soreang, Kota Parepare 91132 Telepon (0421) 21307, Fax. (0421) 24404
PO Box 909 Parepare 91100, website: www.iainpare.ac.id, email: mail@iainpare.ac.id

BERITA ACARA
REVISI JUDUL SKRIPSI

Dekan Fakultas Ekonomi dan Bisnis Islam menyatakan bahwa Mahasiswa:

Nama : NUR AZIZAH
N I M : 2020203861206013
Prodi : Perbankan Syariah

Menerangkan bahwa judul skripsi semula:

DAMPAK SERANGAN VIRUS RANSOMWARE TERHADAP TINGKAT KEPERCAYAAN NASABAHDALAM MENYIMPAN DANA DI BSI KCP BARRU

Telah diganti dengan judul baru:

DAMPAK HOAX TERKAIT ISU SERANGAN VIRUS RANSOMWARE TERHADAP KEPERCAYAAN NASABAH DALAM PENYIMPANAN DANA DI BSI KCP BARRU

dengan alasan / dasar:
.....
.....

Demikian berita acara ini dibuat untuk dipergunakan sebagaimana mestinya.

Parepare, 31 Juli 2024

Pembimbing Utama	Pembimbing Pendamping
Dr. Andi Bahri S., M.E., M.Fil.I.	Dr. Musmulyadi, S.HI., M.M.

Mengetahui;
Dekan,

Dr. Muzdalifah Muhammadun, M.Ag.
NIP. 197102082001122002

KEMENTERIAN AGAMA REPUBLIK INDONESIA
INSTITUT AGAMA ISLAM NEGERI PAREPARE
FAKULTAS EKONOMI DAN BISNIS ISLAM
Jalan Amal Bakti No. 8 Soreang, Kota Parepare 91132 Telepon (0421) 21307, Fax. (0421) 24404
PO Box 909 Parepare 91100, website: www.iainpare.ac.id, email: mail@iainpare.ac.id

Nomor : B.5142/In.39/FEBI.04/PP.00.9/08/2023 30 Agustus 2023
Lampiran : -
Perihal : **Penetapan Pembimbing Skripsi**

Yth: **1. Dr. Andi Bahri S., M.E., M.Fil.I.** **(Pembimbing Utama)**
2. Dr. Musmulyadi, S.HI., M.M. **(Pembimbing Pendamping)**

Assalamu 'alaikum wr. wb.

Berdasarkan hasil sidang judul Mahasiswa (i):

Nama : Nur Azizah

NIM. : 2020203861206013

Prodi. : Perbankan Syariah

Tanggal **19 Juni 2023** telah menempuh sidang dan dinyatakan telah diterima dengan judul:

DAMPAK SERANGAN VIRUS RANSOMWARE TERHADAP TINGKAT KEPERCAYAAN NASABAHDALAM MENYIMPAN DANA DI BSI KCP BARRU

dan telah disetujui oleh Dekan Fakultas Ekonomi dan Bisnis Islam, maka kami menetapkan Bapak/Ibu sebagai **Pembimbing Skripsi** Mahasiswa (i) dimaksud.

Wassalamu'alaikum wr. wb.

Dekan,

Muzdalifah Muhammadun, M.Ag.
NIP. 197102082001122002

Tembusan:
1. Ketua LPM IAIN Parepare
2. Arsip

KEMENTERIAN AGAMA REPUBLIK INDONESIA
INSTITUT AGAMA ISLAM NEGERI PAREPARE
FAKULTAS EKONOMI DAN BISNIS ISLAM
Alamat : JL. Amal Bakti No. 8, Soreang, Kota Parepare 91132 (0421) 21307 (0421) 24404
PO Box 909 Parepare 9110, website : www.iainpare.ac.id email: mail.iainpare.ac.id

Nomor : B-1202/In.39/FEBI.04/PP.00.9/04/2024 17 April 2024
Sifat : Biasa
Lampiran : -
H a l : Permohonan Izin Pelaksanaan Penelitian

Yth. BUPATI BARRU
Cq. Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu
di
KAB. BARRU

Assalamu Alaikum Wr. Wb.

Dengan ini disampaikan bahwa mahasiswa Institut Agama Islam Negeri Parepare :

Nama	: NUR AZIZAH
Tempat/Tgl. Lahir	: PAREPARE, 10 Maret 2002
NIM	: 2020203861206013
Fakultas / Program Studi	: Ekonomi dan Bisnis Islam / Perbankan Syariah
Semester	: VIII (Delapan)
Alamat	: KELURAHAN BUKIT INDAH, KECAMATAN SOREANG, KOTA PAREPARE

Bermaksud akan mengadakan penelitian di wilayah BUPATI BARRU dalam rangka penyusunan skripsi yang berjudul :

DAMPAK SERANGAN VIRUS RANSOMWARE TERHADAP KEPERCAYAAN NASABAH DALAM PENYIMPANAN DANA DI BSI KCP BARRU

Pelaksanaan penelitian ini direncanakan pada tanggal 22 April 2024 sampai dengan tanggal 31 Mei 2024.

Demikian permohonan ini disampaikan atas perkenaan dan kerjasamanya diucapkan terima kasih.

Wassalamu Alaikum Wr. Wb.

Dekan,

Dr. Muzdalifah Muhammadun, M.Ag.
NIP 197102082001122002

Tembusan :

1. Rektor IAIN Parepare

PEMERINTAH KABUPATEN BARRU
DINAS PENANAMAN MODAL DAN PELAYANAN TERPADU SATU PINTU

Mal Pelayanan Publik Masiga Lt. 1-3 Jl. Iskandar Unru Telp. (0427) 21662, Fax (0427) 21410
http://dpmptsptk.barrukab.go.id : e-mail : barrudpmptsptk@gmail.com .Kode Pos 90711

Barru, 22 April 2024

Nomor : 202/IP/DPMPTSP/IV/2024
Lampiran : -
Perihal : Izin Penelitian

Kepada
Yth. Pimpinan Bank Syariah Indonesia KCP Barru

di -
Tempat

Berdasarkan Surat dari Dekan Fakultas Ekonomi dan Bisnis Islam IAIN Parepare Nomor : B-1202/In.39/FEBI.04/PP.00.9/04/2024 perihal tersebut di atas, maka ***Mahasiswi*** di bawah ini :

Nama	**: NUR AZISAH**
Nomor Pokok	**: 2020203861206013**
Program Studi	**: PERBANKAN SYARIAH**
Perguruan Tinggi	**: IAIN PAREPARE**
Pekerjaan	**: MAHASISWI (S1)**
Alamat	**: JL. KEBUN SAYUR KEL. BUKIT INDAH KEC. SOREANG KOTA PAREPARE**

Diberikan izin untuk melakukan Penelitian/Pengambilan Data di Wilayah/Kantor Saudara yang berlangsung mulai tanggal **22 April 2024 s/d 31 Mei 2024,** dalam rangka penyusunan **Skripsi** dengan judul :

DAMPAK SERANGAN VIRUS RANSOMWARE TERHADAP KEPERCAYAAN NASABAH DALAM PENYIMPANAN DANA DI BSI KCP BARRU

Sehubungan dengan hal tersebut diatas, pada prinsipnya kami menyetujui kegiatan dimaksud dengan ketentuan :

1. Sebelum dan sesudah melaksanakan kegiatan, kepada yang bersangkutan melapor kepada Kepala SKPD (Unit Kerja) / Camat, apabila kegiatan dilaksanakan di SKPD (Unit Kerja) / Kecamatan setempat;
2. Penelitian tidak menyimpang dari izin yang diberikan;
3. Mentaati semua Peraturan Perundang Undangan yang berlaku dan mengindahkan adat istiadat setempat;
4. Menyerahkan 1 (satu) eksampelar copy hasil penelitian kepada Bupati Barru Cq. Kepala Dinas Penanaman Modal Dan Pelayanan Terpadu Satu Pintu Kabupaten Barru;
5. Surat Izin akan dicabut kembali dan dinyatakan tidak berlaku apabila ternyata pemegang surat izin ini tidak mentaati ketentuan tersebut di atas.

Untuk terlaksananya tugas penelitian tersebut dengan baik dan lancar, diminta kepada Saudara (i) untuk memberikan bantuan fasilitas seperlunya.

Demikian disampaikan untuk dimaklumi dan dipergunakan seperluhnya.

Kepala Dinas,

Dokumen ini telah ditandatangani secara elektronik
Kepala Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu Kabupaten Barru

ANDI SYUKUR MAKKAWARU, S.STP.,M.Si
Pembina Utama Muda, IV/c
NIP. 19770829 199612 1 001

TEMBUSAN : disampaikan Kepada Yth.
1. Bapak Bupati (sebagai laporan);
2. Kepala Bappelitbangda Kab. Barru;
3. Dekan Fakultas Ekonomi dan Bisnis Islam IAIN Parepare;
4. Mahasiswa yang bersangkutan.

- UU ITE No. 11 Tahun 2008 Pasal 5 Ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah"
- Dokumen ini telah ditandatangani secara elektronik menggunakan setifikat yang diterbitkan BSrE

Balai Sertifikasi Elektronik

PT. Bank Syariah Indonesia, Tbk
Kantor Cabang Pembantu Barru
Jl. A.A. Bau Massepe Ruko UBM
Kel. Mangempang, Kec. Barru, Kab. Barru
90712,Indonesia
T: (0427) 3231755/ 3231741

SURAT KETERANGAN PENELITIAN

No. : 04/ 272 - 03/0121

Yang bertandatangan di bawah ini :

Nama	:	Amiruddin
Jabatan	:	Branch Operations & Service Manager
NIP	:	2189008368

Menerangkan bahwa :

Nama	:	Nur Azizah
NIM	:	2020203861206013
Program Studi	:	Perbankan Syariah
Fakultas	:	Ekonomi dan Bisnis Islam
Perguruan Tinggi	:	Institut Agama Islam Negeri (IAIN) Parepare

adalah benar telah melaksanakan penelitian perihal . DAMPAK HOAX TERKAIT ISU SERANGAN VIRUS RANSOMWARE TERHADAP KEPERCAYAAN NASABAH DALAM PENYIMPANAN DANA DI BSI KCP BARRU.

Demikian surat keterangan ini kami buat dengan sebenarnya untuk dipergunakan sebagaimana mestinya.

Barru, 03 Juli 2024

PT. Bank Syariah Indonesia
***Branch Office* Barru**

Amiruddin
Branch Operations & Service Manager

DOKUMENTASI WAWANCARA

Wawancara dengan pihak Bank Syariah Indonesia Kcp Barru

Wawancara dengan Bapak Amiruddin sebagai *Branch Operation Service Manager* (BOSM) Bank Syariah Indonesia Kcp Barru pada tanggal 24 April 2024

Wawancara dengan Bapak Ardiansyah sebagai *Customer Service* Bank Syariah Indonesia Kcp Barru pada tanggal 24 April 2024

Wawancara dengan Nasabah Bank Syariah Indonesia Kcp Barru

Wawancara dengan Bapak Hamzah sebagai Nasabah Bank Syariah Indonesia Kcp Barru pada tanggal 24 April 2024

Wawancara dengan Julianti sebagai Nasabah Bank Syariah Indonesia Kcp Barru pada tanggal 25 April 2024

BUKTI WAWANCARA

Saya yang bertandatangan dibawah ini:

Nama : AMIRUDDIN

Alamat : JL. TAWAKKAL ROLA

Pekerjaan/ Jabatan : BRANCH OPERATION SERVICE MANAGER (BOSM)

Menyatakan telah di wawancarai oleh:

Nama : NUR AZIZAH

Alamat : JL. ANDI SINTA SELATAN

Pekerjaan : MAHASISWA

Pada : 2

Hari / Tanggal : RABU, 24 APRIL 2024

Waktu : 15.51 - WITA

Tempat : DI BANK SYARIAH INDONESIA (BSI) KCP BARRU

Guna memperoleh data untuk menyelesaikan Skripsi/ Tugas Akhir yang berjudul:

DAMPAK HOAX TERKAIT ISU SERANGAN VIRUS RANSOMWARE TERHADAP KEPERCAYAAN NASABAH DALAM PENYIMPANAN DANA DI BSI KCP BARRU

Demikian keterangan ini di buat, untuk di pergunakan sebagaimana mestinya

Parepare, April 2024

Ttd

BUKTI WAWANCARA

Saya yang bertandatangan dibawah ini:

Nama : ARDIANSYA

Alamat : Jl. Bambu Runcing

Pekerjaan/ Jabatan : CUSTOMER SERVICE

Menyatakan telah di wawancarai oleh:

Nama : NUR AZIZAH

Alamat : JL. ANDI SINTA SELATAN

Pekerjaan : MAHASISWA

Pada :

Hari / Tanggal : RABU, 24 APRIL 2024

Waktu : 14.49. WITA

Tempat : DI BANK SYARIAH INDONESIA (BSI) KCP BARRU

Guna memperoleh data untuk menyelesaikan Skripsi/ Tugas Akhir yang berjudul:

DAMPAK HOAX TERKAIT ISU SERANGAN VIRUS RANSOMWARE TERHADAP KEPERCAYAAN NASABAH DALAM PENYIMPANAN DANA DI BSI KCP BARRU

Demikian keterangan ini di buat, untuk di pergunakan sebagaimana mestinya

Parepare, April 2024

Ttd Ardiansya

BUKTI WAWANCARA

Saya yang bertandatangan dibawah ini:

Nama : HAMIAH

Alamat : MANGKOSO, SOPPENG RIAJA, BARRU

Pekerjaan/ Jabatan : PEGAWAI KANTOR KEMENTERIAN AGAMA KAB. BARRU

Menyatakan telah di wawancarai oleh:

Nama : NUR AUZAH

Alamat : JL. ANDI SINTA SELATAN

Pekerjaan : MAHASISWA

Pada

Hari / Tanggal : BARRU, 24 APRIL 2024

Waktu : 14.33 WITA

Tempat : DI BANK SYARIAH INDONESIA (BSI) KCP BARRU

Guna memperoleh data untuk menyelesaikan Skripsi/ Tugas Akhir yang berjudul:

DAMPAK HOAX TERKAIT ISU SERANGAN VIRUS RANSOMWARE TERHADAP KEPERCAYAAN NASABAH DALAM PENYIMPANAN DANA DI BSI KCP BARRU

Demikian keterangan ini di buat, untuk di pergunakan sebagaimana mestinya

Parepare, April 2024

Ttd

BUKTI WAWANCARA

Saya yang bertandatangan dibawah ini:

Nama : JULIANTI

Alamat : LAPAKAKA, BARRU

Pekerjaan/ Jabatan : MAHASISWA

Menyatakan telah di wawancarai oleh:

Nama : NUR AZIZAH

Alamat : JL. ANDI SINTA SELATAN

Pekerjaan : MAHASISWA

Pada : 25 APRIL 2024

Hari / Tanggal : KAMIS, 25 APRIL 2024

Waktu : 15- 30 WITA

Tempat : LAPAKAKA, BARRU (Rumah Nasabah)

Guna memperoleh data untuk menyelesaikan Skripsi/ Tugas Akhir yang berjudul:

DAMPAK HOAX TERKAIT ISU SERANGAN VIRUS RANSOMWARE TERHADAP KEPERCAYAAN NASABAH DALAM PENYIMPANAN DANA DI BSI KCP BARRU

Demikian keterangan ini di buat, untuk di pergunakan sebagaimana mestinya

Parepare, April 2024

Ttd

BIODATA PENULIS

Nama Penulis Nur Azizah, lahir pada tanggal 10 Mart 2002. Alamat Jl, Andi Sinta Selatan, Kecamatan Soreang, Kelurahan Ujung, Kota Parepare, Sulawesi Selatan. Anak Bungsu, Ayah bernama Muh Hafid dan Ibu bernama Maminasa.

Adapun riwayat hidup pendidikan penulis memulai masuk Sekolah Dasar Negeri 18 Parepare dan selesai pada tahun 2014. Selanjutnya penulius masuk Sekolah Menengah Pertama Negeri 2 Parepare dan selesai pada tahun 2017. Kemudian melanjutkan jenjang pendidikan SMA Negeri 1 Parepare dan selesai pada tahun 2020. Kemudian melanjutkan S1 di Institut Agama Islam Negeri Parepare pada tahun 2020, dengan mengambil Program Studi Perbankan Syariah Fakultas Ekonomi dan Bisnis Islam. Pada semester 5, penulis mengikuti Program MBKM (Merdeka Belajar Kampus Merdeka) yang dirangkaikan langsung dengan Praktik Pengalaman Lapangan dan Praktikum Bank Mini di Bank Syariah Indonesia KCP Barru. Penulis melaksanakan Kuliah Pengabdian Masyarakat (KPM) tahun 2023 di Desa Singki Kecamatan Anggeraja, Kabupaten Enrekang. Hingga penulis menyelesaikan studi dengan mengambil judul skripsi.

"Dampak Hoax Terkait Isu Serangan Virus *Ransomware* Terhadap Kepercayaan Nasabah Dalam Penyimpanan Dana Di BSI Kcp Barru"