TESIS

FORMULA MODEL PENANGANAN PHISHING PADA BANK BRI: ANALISIS, DAMPAK, DAN IMPLEMENTASI

disusun dan diajukan oleh

FITRI QALABI ILYAS

A012221063

kepada

PROGRAM MAGISTER MANAJEMEN

FAKULTAS EKONOMI DAN BISNIS

UNIVERSITAS HASANUDDIN

2023

LEMBAR PENGESAHAN TESIS

FORMULA MODEL PENANGANAN PHISING PADA BANK BRI: ANALISIS, DAMPAK, DAN IMPLEMENTASI

Disusun dan diajukan oleh:

FITRI QALABI ILYAS
NIM A012221063

Telah dipertahankan di hadapan Panitia Ujian yang dibentuk dalam rangka Penyelesaian Studi Program Magister Program Studi Manajemen Fakultas Ekonomi dan Bisnis Universitas Hasanuddin pada tanggal **16 Februari 2024** dan dinyatakan telah memenuhi syarat kelulusan

Menyetujui,

Pembimbing Utama	Pembimbing Pendamping
Dr. Muhammad Sobarsyah, SE., M.Si.	**Dr. Fauzi R. Rahim, SE., M.Si., CSF., AEPP**
NIP 196806291994031002	**NIP 196503141994031001**

Ketua Program Studi Magister Manajemen	Dekan Fakultas Ekonomi dan Bisnis Universitas Hasanuddin
Dr. H. Muhammad Sobarsyah, S.E., M.Si.	**Prof. Dr. H. Abd.Rahman Kadir., S.E., M.Si., CIPM.**
NIP 196806291994031002	**NIP 196402051988101001**

PERNYATAAN KEASLIAN

Yang bertanda tangan di bawah ini

Nama	: Fitri Qalabi Ilyas
Nim	: A012221063
Program studi	: Magister Manajemen
Jenjang	: S2

Menyatakan dengan ini bahwa Tesis dengan **Formula Model Penanganan Phishing Pada Bank BRI: Analisis, Dampak, dan Implementasi**

Adalah karya saya sendiri dan tidak melanggar hak cipta pihak lain. Apabila di kemudian hari Tesis karya saya ini terbukti bahwa sebagian atau keseluruhannya adalah hasil karya orang lain yang saya pergunakan dengan cara melanggar hak cipta pihak lain, maka saya bersedia menerima sanksi

Makassar, 8 Maret 2024

Yang Menyatakan,

Fitri Qalabi Ilyas

ABSTRAK

FITRI QALABI ILYAS. Formula Model Penanganan Phising Pada Bank BRI: Analisis, Dampak, dan Implementasi (dibimbing oleh Sobarsyah dan Fauzi R. Rahim)

Phising merupakan salah satu jenis serangan siber dengan meniru alamat website asli lalu menyebarkannya melalui pesan Whatsapp, telepon maupun email. Tujuan tindakan serangan phishing yaitu untuk mengetahui informasi data sensitive masyarakat seperti username, password, ccv, masa berlaku kartu kredit, dan lain-lain yang tujuan akhirnya untuk memperoleh keuntungan finansial bagi pelaku, sehingga menyebabkan kerugian finansial terhadap korban dan perusahaan. Metodologi yang digunakan adalah metode kualitatif dengan menggunakan teknik pendekatan studi literatur dengan bantuan analisis matriks risiko, analisis skenario dan analisis bow tie risk. Penulis menemukan bahwa akar masalah dari tingginya serangan phising pada bank BRI adalah Kerentanan manusia yang dikibatkan oleh kecerobohan dan kurangnya pengetahuan membuat penipuan phising mengalami peningkatan. Dari segi teknologi yaitu tidak terdapat alat deteksi phising dan peringatan ketika terjadi pemindahan dana rekening ke rekening yang tidak dikenal. Untuk meminimalisir akar masalah yang dihadapi maka diperlukan formulasi model penanganan phising yang lebih efektif dibanding sebelumnya. Formulasi model penangan yang tepat untuk mengurangi serangan phising yaitu meningkatkan pengetahuan dan kesadaran nasabah khususnya 40 tahun keatas melalui simulasi secara langsung. Selain itu, perlu dilakukan peningkatan sistem teknologi yang canggih berupa pengembangan sistem teknologi yang dapat mendeteksi serangan phising serta memberi peringatan secara real time jika terdapat pemindahan dana yang mencurigakan.

Kata Kunci: *phishing, analisis matriks risiko, skenario what-if, bow tie risk*

ABSTRACT

FITRI QALABI ILYAS. Formulation of Phishing Handling Model at BRI Bank: Analysis, Impact, and Implementation (supervised by Sobarsyah and Fauzi R. Rahim)

Phishing is a type of cyber attack by imitating the original website address and then distributing it via Whatsapp messages, telephone or email. The aim of phishing attacks is to find out people's sensitive data information such as usernames, passwords, ccv, credit card validity periods, and others whose ultimate goal is to gain financial benefits for the perpetrators, causing financial losses to victims and companies. The methodology used is a qualitative method using a literature study approach technique with the help of risk matrix analysis, scenario analysis and bow tie risk analysis. The results show that root cause of the high number of phishing attacks on BRI bank is human vulnerability caused by carelessness and lack of knowledge, which has increased phishing fraud. In terms of technology, there are no phishing detection tools and warnings when there is a transfer of account funds to an unknown account. To minimize the root of the problem faced, it is necessary to formulate a phishing handling model that is more effective than before. The formulation of the right handling model to reduce phishing attacks is to increase customer knowledge and awareness, especially 40 years and over through direct simulation. In addition, it is necessary to improve sophisticated technology systems in the form of developing technology systems that can detect phishing attacks and provide real-time warnings if there is a suspicious transfer of funds.

Keywords: Phishing, risk matrix analysis, what-if scenario, bow tie risk.

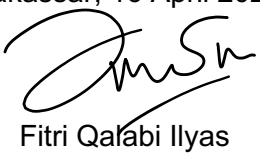
PRAKATA

Puji syujur atas kehadirat Allah SWT atas limpahan rahmat dan hidaya-Nya, sehingga penulis dapat melaksanakan dan menyelesaikan penyusunan tesis yang berjudul “Formula Model Penanganan Phising Pada Bank BRI: Analisi, Dampak, dan Implementasi”. Penulisan tesis ini disusun sebagai salah satu persyaratan untuk menyelasikan studi dan memperoleh gelar Magister Manajemen di Universitas Hasanuddin Makassar. Selama proses penyusunan tesis ini, terdapat berbagai macam kesulitan yang dihadapi oleh peneliti, akan tetapi kesulitan dan hambatan tersebut dapat penulis lewati dengan baik berkat tekad yang kuat, doa, dukungan, dan bimbingan yang didapatkan dari berbagai pihak. Oleh karena itu, peneliti menyampaikan rasa terima kasih yang setulusunya kepada pihak yang telah membantu dalam proses penyusunan skripsi baik secara langsung maupun secara virtual. Ucapan terimakasih peneliti hanturkan kepada:

1. Allah Subhanahu Wa Ta'ala, atas izin dan karunia-Nya dapat terselesaikannya tesis ini.
2. Nabi Muhammad SAW yang senantiasa memberikan syafaat bagi umat-Nya
3. Kedua orangtua Ayahanda H. Muh. Ilyas Quddus dan Ibunda Hj. Nurlina yang senantiasa mendoakan, memberikan dukungan, dan kasih sayang yang tiada hentinya kepada penulis.
4. Dr. Muhammad Sobarsyah , SE.,M.Si selaku Dosen Pembimbing I dan Bapak Dr. Fauzi R. Rahim, SE., M.Si, selaku Dosen Pembimbing II terimakasih telah meluangkan waktu dan tenaga serta memberikan bimbingan, saran, arahan, dan dukungan kepada penulis dalam proses penyusunan tesis.
5. Prof. Dr. H. Rahkman Laba, SE.,MBA selaku dosen penguji I, Prof. Dr. H. Cepi Pahlevi , SE.,M.Si selaku penguji II, dan Dr. Andi Aswan., SE., MBA., M.Phil., DBA selaku dosen penguji III, terima kasih atas saran serta nasihat dan bimbingan yang diberikan kepada penulis.
6. Semua pihak yang membantu dalam penyusunan tesis dan tidak dapat peneliti sebutkan satu persatu.

Semoga Allah SWT, membalas segala kebaikankan, doa, dukungan, serta bantuan yang diberikan kepada peneliti selama menjadi Mahasiswi di Universitas Hasanuddin. Penulis menyadari bahwa dalam penulisan ini terdapat kesalahan dan kekurangan. Oleh karena itu, kritik dan saran sangat diharapkan kepada penulis demi perbaikan penelitian selanjutnya. Semoga penelitian ini dapat bermanfaat bagi pembaca.

Makassar, 16 April 2024



Fitri Qalabi Ilyas

DAFTAR ISI

USULAN PENELITIAN TESIS i
HALAMAN PERSETUJUAN ..... **Error! Bookmark not defined.**
DAFTAR ISI viii
DAFTAR TABEL iv
BAB I PENDAHULUAN 1
1.1 Latar belakang 1
1.2 Profil Bank Rakyat Indonesia 5
1.3 Masalah bisnis 7
1.4 Pertanyaan penelitian 7
1.5 Tujuan penelitian 7
BAB II EKSPLORASI MASALAH 8
2.1 Ekosistem phishing ..... **Error! Bookmark not defined.**
2.2 Analisis internal phising 21
2.3 Analisis matriks risiko 22
2.4 Analisis skenario 23
2.5 Analisis bow tie risk 24
2.6 Kondisi keuangan perusahaan 25
BAB III SOLUSI 28
3.1 Analisis maktris risiko 28
3.2 Analisis skenario 33
3.3 Analisis bow tie risk 36
3.4 Perumusan strategi 41
BAB IV PENUTUP 45
4.1 Rencana implementasi 45
4.2 Kesimpulan 48
DAFTAR PUSTAKA 50

DAFTAR TABEL

Tabel 1. 1 Cyber-attack by industry 1
Tabel 1. 2 Tren phising perbankan Indonesia 3
Tabel 2. 1 Kasus phising nasabah bank BRI 13
Tabel 2. 2 Skala probabilitas matriks risiko 22
Tabel 2. 3 Skala dampak matriks risiko 23
Tabel 2. 4 Beban operasional Bank BRI 27
Tabel 3. 1 Kasus phising bank BRI yang teridentifikasi 28
Tabel 3. 2 Kategorisasi kemungkinan 30
Tabel 3. 3 Risk matrix 31
Tabel 3. 4 what-if:increase financial impact 33
Tabel 3. 5 Skenario peningkatan dampak 34
Tabel 3. 6 what-if: Peningkatan keamanan dan kesadaran nasabah 35
Tabel 3. 7 Skenario peningkatan keamanan dan kesadaran nasabah 35
Tabel 3. 8 what-if: Peraturan lebih ketat dan pemberian kompensasi 36

DAFTAR GAMBAR

Gambar 2. 1 Phishing ecosystem 17
Gambar 2. 2 Contoh phising 19
Gambar 2. 3 BRIMO phising 20
Gambar 3. 1 Bow tie analysis 40

BAB I
PENDAHULUAN

1.1 Latar belakang

Distrupsi digital menjadi tantangan sebuah bisnis di era revolusi industry 4.0 di mana serangan siber berkembang dengan pesat yang menjadi ancaman serius pada sebuah organisasi khususnya pada sektor perbankan. Kejahatan siber dalam dunia perbankan menjadi hal yang perlu diperhatikan, mengingat sektor keuangan memiliki sistem jaringan yang sangat kompleks dan saling terhubung sehingga menjadi target utama serangan siber. Data sensitif seperti informasi keuangan dan data pribadi nasabah yang disimpan oleh industri perbankan menjadikan sasaran menarik bagi penjahat siber yang ingin mencapai keuntungan finansial.

Tabel 1. 1 Cyber-attack by industry

	%				
Cyber-attack by industry	**2018**	**2019**	**2020**	**2021**	**2022**
Manufacturing	10	8	17,7	23,2	24,8
Finance and Insurance	19	17	23	22,4	18,9
Professional, business and consumer services	12	10	8,7	12,7	14,6
Energy	6	6	11,1	8,2	10,7
Retail and wholesale	11	16	10,2	7,3	8,7
Education	6	8	4	2,8	7,3
Healthcare	6	3	6,6	5,1	5,8
Government	8	8	7,9	2,8	4,8
Transportation	13	13	5,1	4	3,9
Media and telecom	8	10	5,7	2,5	0,5

Sumber: IBM, 2023

Tabel 1.1 merupakan persentase serangan yang paling banyak terjadi berdasarkan sektor industry. Pada tabel di atas menggambarkan bahwa serangan siber yang paling banyak terjadi yaitu pada industri manufaktur dan industri keuangan dan asuransi. Industri keuangan dan asuransi menjadi industri

yang paling menjadi sasaran serangan siber dari tahun 2018-2020. Analisis lebih lanjut dari laporan yang dikeluarkan oleh IBM bahwa serangan pada industri keuangan dan asuransi lebih spesifik banyak terjadi pada organisasi perbankan yaitu sebesar 70%, organisasi asuransi 16%, dan 14% lainnya berasal dari organisasi keuangan lainnya. Jika dirincikan lebih lanjut dengan asumsi bahwa sektor perbankan menyumbang sebesar 70% tiap tahun, maka sektor perbankan mengalami serangan siber sebesar 13,3% pada tahun 2018, tahun 2019 sebesar 11,9%, tahun 2020 16,1%, tahun 2021 sebesar 15,68%, dan tahun 2022 sebesar 13,23%.

Risiko serangan siber memberikan dampak yang akan mempengaruhi kerahasiaan, ketersediaan, integritas, hinggga sistem informasi (Cebula and Young, 2010). Dengan arti lain bahwa, serangan siber akan menganggu sistem operasional bank yang akan mengancam keamanan data nasabah, integritas transaksi, dan stabilitas sistem finansial. Seperti yang kita tahu, bahwa bank memproses miliaran transkasi uang tiap harinya melalui jaringan yang menandakan bahwa sektor perbankan menjadi sektor yang paling vital terkena serangan siber. Terdapat beberapa serangan siber yang sering terjadi pada perbankan salah satunya yaitu jenis serangan phising yang dapat terjadi pada bank maupun nasabah bank itu sendiri.

Phising merupakan salah satu jenis serangan siber dengan meniru alamat website asli lalu menyebarkannya melalui pesan Whatsapp, telepon maupun email. Tujuan tindakan serangan phishing yaitu untuk mengetahui informasi data sensitive masyarakat seperti username, password, ccv, masa berlaku kartu kredit, dan lain-lain yang tujuan akhirnya untuk memperoleh keuntungan. Secara singkat, tindakan phishing melalui tiga tahap secara mendasar yaitu pembuatan website yang sangat mirip dengan website asli, lalu mengalihkan koneksi situs website tersebut melalu saluran komunikasi, dan terakhir yaitu pencurian identitas para korban.

Anti-Phishing working Group (APWG) mendefinisikan phishing sebagai metode kejahatan yang menggunakan *social engineering* dan kecanggihan teknologi untuk memperoleh keuntungan. Serangan phishing ini sangat

bergantung pada rekayasa sosial teknologi yang menjadi pondasi utama untuk melakukan serangan phishing. Menurut *Federal Trade Commisions* (FTC), phishing merupakan jenis penipuan online yang menargetkan konsumen dengan mengirimkan email dengan tampilan seperti email resmi dari suatu organisasi. Menurut strategi dan keamanan siber inggris dan statistic 2016-2021 bahwa hampir semua serangan siber yang terjadi tidak terlepas dari peran manusia. Artinya, kejadian ini tidak hanya disebabkan oleh teknologi akan tetapi pengetahuan mengenai keamanan sangat diperlukan dalam stabilitas keamanan siber. Dari definisi diatas maka dapat disimpulkan bahwa phishing merupakan kejahatan siber dengan menjebak pengguna ke situs website yang secara visual sama dengan situs website resmi organisasi.

Tabel 1. 2 Tren phising perbankan Indonesia

TREN PHISING PERBANKAN INDONESIA		
Tahun	**Periode**	**Total serangan**
2022	kuartal I	1113
	kuartal II	615
	kuartal III	2305
	kuartal IV	1601
2023	kuartal I	5783
	kuartal II	2776
	kuartal III	1563

Sumber: IDADX, 2023

Berdasarkan data dari IDADX (Indonesia Anti Phishing Data Exchage) melaporkan bahwa tren phising khususnya pada perbankan Indonesia masih relatif tinggi. Pada tabel 1.2 dapat dilihat bahwa total jumlah serangan pada tahun 2022 sebesar 5.634 serangan dan pada tahun 2023 total jumlah serangan sampai kuartal 3 yaitu 10.122. Hal ini disebakan karena para pelaku serangan siber menggunakan teknik phising yang semakin canggih dan relevan dengan kehidupan sehar-hari. Deputi Bidang Pengembangan, Riset Terapan, Teknik dan PANDI mengatakan bahwa tingginya kasus phising pada tahun 2023 dibanding dengan tahun sebelumnya karena para pelaku menggunakan domain protocol HTTPS, sehingga masyarakat mudah percaya karena menganggap bahwa

domain tersebut merupakan doamin yang terpercaya dan mudah untuk diakses. Badan Siber dan Sandi Negara juga mencatat bahwa jumlah serangan siber mengalami peningkatan yang cukup besar dari pada tahun 2021 sebesar 266,7 juta dan pada tahun 2022 sebesar 370 juta. Dan sebanyak 33.305.209 aktivitas yang mencurigakan yang terdeteksi dari situs phishing. Hal ini mengindikasikan bahwa ini menjadi hal sangat penting untuk diperhatikan.

Di Indonesia terdapat beberapa macam Bank, salah satu bank tersebut adalah Bank BRI. Bank BRI merupakan bank yang memiliki asset terbesar di Indonesia dengan jumlah asset mencapai Rp. 1.416,8 triliun pada tahun 2019. Hingga pada tahun 2022, total asset terus mengalami peningkatan dengan total asset sebesar Rp.1.865,6 triliun. Selain menjadi bank yang memiliki asset terbesar di Indonesia, bank BRI juga memilik jumlah nasabah terbanyak di Indonesia. Sebagai bank yang memiliki nasabah terbanyak di Indonesia, bank BRI memiliki peran penting dalam menjaga kepercayaan nasabah terkait data pribadi. Dikarenakan bank BRI memiliki nasabah terbanyak, tentunya bank BRI dihadapakan risiko khususnya risiko keamanan siber.

Terdapat beberapa kasus yang sedang marak terjadi pada nasabah bank BRI terkait serangan phishing yang mengatasnamakan pihak resmi bank BRI. Modus pelaku phising melalui via telefon dengan mengatasnamakan pihak bank BRI dengan suara yang khas mirip dengan *costumer service* BRI yang memberikan penyampaian kepada korban bahwa adanya perubahan biaya tarif transfer lalu pelaku mengirimkan link phising kepada korban melalui via SMS. Dari link phising tersebut, korban kemudian diarahkan ke website dengan tampilan yang sangat mirip dengan aplikasi mobile banking BRIMO yang asli, mulai dari design, logo, dan domain yang diberikan. Sehingga, korban tidak merasa curiga dari link phising tersebut. Hingga pada akhirnya, korban mengetik username dan password untuk login ke link tersebut. Ketika korban mengecek saldo di rekeningnya saldonya telah hilang tanpa kode OTP. Berbeda dengan modus pelaku sebelumnya, modus pelaku pada kasus ini yaitu mengaku sebagai kerabat terdekat korban dan mengirimkan sebuah undangan digital berbentuk file APK yang didalam file tersebut berisi *malware* yang berbahya. Virus *malware* tersebut

dapat mencuri data dari jarak jauh termasuk data *internet banking* yang ada di handphone. Ketika korban mengklik file undangan yang berisi malware tersebut, tanpa disadari saldo yang direkening hilang.

Kasus phishing yang sering terjadi juga mengindikasikan bahwa adanya kebocaran data nasabah dan kurangya kewaspadaan terkait serangan phising. Oleh karena itu, penting bagi perbankan untuk mengatahui penyebab terjadinya phising yang dialami oleh nasabah. Sehingga Model penanganan phising perlu dikembangkan mengingat serangan digital semakin berkembang seiring dengan kecanggihan teknologi. Oleh karena itu diperlukan untuk menganalisis lebih lanjut mengenai model penganganan phising untuk melindungi asset dan informasi nasabah serta menjaga kepercayaan nasabah kepada bank BRI.

1.2 Profil Bank Rakyat Indonesia

Bank Rakyat Indonesia didirikan pada tanggal 16 Desember 1895 oleh Raden Bei Aria Wirjaatmadja di Purwekerto, Jawa tengah yang memiliki visi untuk memajukan perekonomian Indonesia melalui peningkatakan kesejahteraan masyarakat Indonesia. Visi untuk memajukan perekonomian Indonesia melalui peningkatakan kesejahteraan masyarakat Indonesia menjadi fokus utama yang senantiasa memberikan pelayanan kepada segmen usaha, baik dari segi usaha mikro, kecil, hingga menengah (UMKM). Melalui program dalam memajukan ekonomi masyarakat, jumlah nasabah UMKM BRI terus mengalami peningkatan tiap tahunnya. Dan dengan komitmen yang penuh dalam memberikan pelayanan prima serta kerja yang optimal menjadikan Bank BRI sebagi bank yang memiliki asset terbesar di Indonesia dengan jumlah asset mencapai Rp. 1.416,8 triliun pada tahun 2019. Hingga pada tahun 2022, total asset terus mengalami peningkata dengan total asset sebesar Rp.1.865,6 triliun. Ditengah pergeseran perilaku masyarakat yang serba digital, bank BRI memanfaatkan hal tersebut melalui transformasi digital dengan meluncurkan berbagai produk digital seperti BRImo, BRI smart billing, Ceria, BRIguna digital, serta produk-produk digital turunannya. Dengan peluncuran produk digital tersebut, tercatat hingga akhir

tahun 2022 BRIMO telah di diunduh lebih dari 23,8 juta pengguna dan menghasilkan lebih dari 1,8 miliar transaksi pada aplikasi mobile banking.

Pertumbuhan pengguna digitalisasi perbankan pada bank BRI tentunya tidak terlepas dari pengelolan sistem keamanan data konsumen. Dalam transformasi digitalnya bank BRI menerapkan beberapa regulasi terkait dalam pengamanan dan pengelolaan data nasabah yang dituangakan dalam beberapa regulasi yaitu UU No Tahun 1998 tentang Perbankan, PP No 71 Tahun 2019 tentang Penyelangaraan Sistem dan Transaksi Elektronik, POJK No 38/POJK.03/2016 tentang Penerapan Manajemen risiko dalam penggunanaan teknologi informasi oleh bank umum, serta SE OJK N0. 14/SEOJK.07/2014 tentang kerahiasaan dan keamanan data dan/atau informasi pribadi konsumen, Surat Ederan Internal tentang pengamanan data nasabah, petunjuk pelaksanaan rahasia bank dan pelaporan pihak ketiga serta surat edaran internal terkait penerapan dan penggunaan formulir utama nasabah.

Dari sisi sistem keamanan bank BRI, bank BRI memiliki kebijakan *cyber security* yang mengatur mengenai kemanan informasi BRI secara *bank-wide.* Kebijakan yang diterapkan disusun berdasarkan standar internasional ISO270001:2013, PCI DSS (*payment card industry data security standard*). Untuk melindungi aplikasi mobile yang dimiliki oleh bank BRI, bank BRI menerapkan teknologi *Mobile Apps Security*. Penerapan teknologi *Mobile Apps Security* bertujuan agar aplikasi bisa lebih tahan terhadap serangan siber. Dalam pengembangan tiap aplikasi yang dibuat, mulai dari tahap desain, pengembangan, hingga pengujian aplikasi bank BRI menerapkan *security shift left.* Sehingga untuk mengontrol ancaman siber, bank BRI memiliki bagian khusus yang secara terus menerus akan mengawasi selama 24 jam,setiap minggu selama 365 hari dan BRI juga melakukan pengawasan secara proaktif menggunakan layanan *threat hunting* dan *threat intelligence service* yang telah dikembangjan dengan memasukkan dalam *provider* yang berskala internasional. Akan tetapi disamping sistem keamanan yang dimiliki oleh bank BRI, bank BRI memiliki risiko serangan siber yang sering terjadi pada nasabahnya. Jenis serangan siber yang sering terjadi pada nasabahnya yaitu serangan phising. Dari kasus yang teridentifkasi,

terdapat 11 kasus phising dengan total kerugian hampir 5,8 Miliar. Kasus dengan jumlah kerugian paling besar banyak terjadi pada tahun 2023. Hal ini menunjukkan bahwa kasus phising pada nasabah bank BRI mengalami peningkatan dengan dampak yang besar bagi nasabah. Oleh karena itu, bank BRI perlu melakukan tindakan untuk mengurangi serangan phising yang terjadi.pada nasabah.

1.3 Masalah bisnis

Bank BRI sebagai bank yang memiliki nasabah terbanyak memiliki kerentanan yang lebih tinggi terkait serangan siber utamanya serangan phising. Dari beberapa kasus yang telah terjadi banyak nasabah yang beranggapa bahwa tanggapan yang diberikan oleh bank di nilai lambat. Sehingga dari kejadian tersebut kepercayaan nasabah terkait bank BRI menurun akibat banyaknya kasus phising yang terjadi pada nasabah BRI dan hal ini juga pastinya akan berdampak pada finansial bank BRI.

1.4 Pertanyaan penelitian

Berdasarkan objek masalah diatas, pertanyaan utama kana mengacu pada formulasi model penanganan phising yang akan dihasilkan pada fase selanjutnya. Pertanyaan spesifiknya adalah:

1. Apa penyebab utama tingginya serangan phising pada bank BRI?
2. Apa formulasi model penanganan yang terbaik yang dapat diterapkan pada bank BRI dalam menangani phising?

1.5 Tujuan penelitian

Berdasarkan pertanyaan, maka tujuan dari penelitian ini:

1. Untuk menganalisis penyebab utama meningkatnya serangan phising
2. Untuk menciptakan formulasi model penanganan phising pada bank BRI

BAB II
EKSPLORASI MASALAH

2.1 Phising

Phising merupakan tindakan penyalahgunaan untuk mengakses informasi dan data pengguna yang tidak sah. Phising pada layanan publik menjadi ancaman rekayasa sosial yang rentan terjadi, seperti halnya pada layanna perbankan online. Menurut lanskap keamanan siber Indonesia mengungkapkan bahwa selama tahun 2022 kasus aplikasi phising perbakna semakin meningkat yang menargetkan nasabag perbakan untuk mendapatkan nomor pin rekening dan kode OTP korban. Menurut APWG (2018), phising merupakan mekanisme kejahatan yang menggunakan teknik rekayasa sosial dengan teknik penelabuan untuk mengambil informasi data pribadi pengguna dan juga mengambil data akun keuangan korban. Selain itu, US-CERT juga mendefinisikan phising sebagai bentuk rekayasa sosial yang menggunakan email dan situs berbaya dalam aksinya untuk mengumpulkan informasi data pribadi baik secara individual maupun memproleh dari perusahaan dengan modus pelaku berpura-pura sebagai organisasi atau entitas yang dipercaya. Badan Siber dan Sandi Negara mendefinisikan phising sebagai kejahatan sibier dengan memanfaatkan aplikasi website palsu dengan tampilan yang sangat mrip dengan aplikasi resmi yang bertujuan untuk mengelabui korban agar korba percaya untuk memberikan dan memasukkan data rahasis seperti *username* dan *password,* nomor pin, melakukan instalasi aplikasi berbahaya, dan lain-lain. Terdapat beberapa jenis tujuan motif serangan phising dilakukan yaitu untuk keuntungan finansial, pencurian data penting informasi pengguna, dan merusak citra perusahaan terkait. Seseorang menjadi sasaran yang paling rentan terkena serangan penipuan online seperti phising dengan metode rekayasa sosial karena kuranganya kesadaran individu dalam melindungi data informasi rahasia serta kurangnya pengetahuan tentang keamana data pengguna. Menurut Luga (2016) kebanyakan kasus phising terjadi karena kesalahan alami pengguna itu sendiri jika dibandingkan dengan kecanggihan teknologi. Hal ini juga dikemukakan oleh Alsaedam (2013), bahwa kurangnya pengetahuan, perolehan informasi yang

terbatas, dan kecenderungan korban itu sendiri nmenjadi penyebab terjadi phising. Faktor manusia dalam hal perilaku dan faktor psikologis mempengaruhi tingkat keberhasilan serangan phising yang terjadi. Menurut Hakim (2020) yang melakukan percobaan phising berbasi laboratorium dalam kehidupan nyata mengemukakan bahwa lebih dari 30% yang telah diuji mengklik sebuah tautan berbaya dan kebanyakan dari mereka tidak ragu memberikan username dan kata sandi.

2.2 Jenis-jenis phising

Phising mengalami pertumbuhan yang signifikan ditengah era serba digital sehingga hal ini menjadi perhatian khusus. Phising memimiliki beberapa jenis diantaranya rekayasa sosial phising, phising berbasis DNS, phising bebrbasis ijeksi konten, dan lain-lain yang akan dijelaskan dibawah ini:

2.2.1 Rekayasa sosial phising

Rekayasa sosial phising meliputi bebrapa aktivitas untuk mengeksploitasi atau memanfaatkan kesalahan manusia atau perilaku manusia untuk memperoleh akses informasi yang sensitive dari kecerobahan korban. Pelaku menggunakan beberapa teknik untuk memanipulasi korban untuk mengambil alih informasi rahasia. Dalam keamanan siber, rekayasa sosial merupakan upaya yang dilakukan oleh pelaku dalam membujuk pengguna agar memberikan informasi sensitif, membuka dokumen, file atau email, membuka website yang telah terinfeksi virus malware. Rekayasa sosial phising merupakan jenis penipuan yang memanfaatkan kelemahan manusia untuk mengakses informasi yang tidak sah dari pengguna. Metode ini sering kali digunakan dalam penipuan karena metode yang mudah untuk memanfaatkan kebiasaan yang buruk dari pengguna yaitu memiliki sistem keamanan yang dimiliki sangat lemah. Selain itu, menurut Univeristy of Minnesota (2019) bahwa seseorang sering menjadi korban penipuan secara online karena faktor psikologi yang mengontrol emosi yang kuat pada manusia seperti rasa takut, rasa ingin tahu, bantuan, hal darurat.

2.2.2 Phising berbasis DNS

Pharming merupakan sebutan lain dari phising berbasis DNS. Jenis serangan ini menggunakan jaringan komputer untuk meretas jaringan korban menggunakan virus atau malware untuk mengalihkan jaringan lalu lintas korban ke situs yang berbahaya. Hal ini dilakukan penyerang untuk mendapatkan informasi data pengguna secara tidak sah. Menurut Darmawan (2023), serangan pharming merupakan serangan yang dikendalikan oleh pelaku penyerang untuk mengalihkan lalu lintas jaringan internet dari situs website resmi ke situs website palsu. Dalam hal layanan perbankan berbasis online, jenis serangan ini menyebabkan penggunan dialihkan ke situs website palus yang tampilan website tersebut sangat mirip dengan situs wesite resmi perbankan, sehingga hal ini akan membuat pengguna tidak menaruh curiga memasukkan data informasi yang diminta dalam website palsu tersebut seperti *username* dan *password* pengguna.

2.2.3 Phising berbasis proksi

Proksi merupakan sebuah server yang bertindak sebagai perantara antara internet dan komputer. Proksi memiliki fungsi dasar yaitu sebagai server yang menyimpan konten situs website dalam bentuk cache untuk mempercepat pengguna dalam mengakses sebuah laman yang diinginkan. Serangan phising berbasis proksi ini memungkinakan pelaku untuk mencuri nama pengguna dan kata sandi ketika arahan permintaan pengguna menuju laman yang diinginkan atau meretas sesi yang sudah diautentikasi dengan menggunakan cookie korban.

2.2.4 Phising berbasis DHCP

Dynamic Host Configuration Protocol (DHCP) dikembangkan pada tahun 1900-an yang berfungsi untuk menyederhanakan pemeliharaan dan konfigurasi jaringan. DHCP ini merupakan protokol manajemen jaringan yang mengizinkan setiap perangkat dalam jaringan untuk berkomunikasi dengan jaringan IP lainnya sehingga memiliki alamat IP yang dinamis dengan parameter jaringan lainnya. Serangan jenis ini menggunkan

alamat MAC palsu untuk meminta alamat IP server DHCP. Pelaku penyerang akan menetapkan beberapa alamat MAC sumber yang telah dipalsukan dan menyebarkan dengan jumlah yang besar dalam bentuk DHCP REQUEST ke server dalam serangan DHCP. Dalam waktu yang singkat, server ini mulai menerima permintaan kemudian akan mulai merespons dengan alamat yang IP yang tersedia. Pelaku penyerangan jenis ini akan membuat server DHCP yang berbahaya kemudian penyeran akan melakukan serangan selanjutnya yaitu serangan spoofing.

2.2.5 Phising berbasis injeksi konten

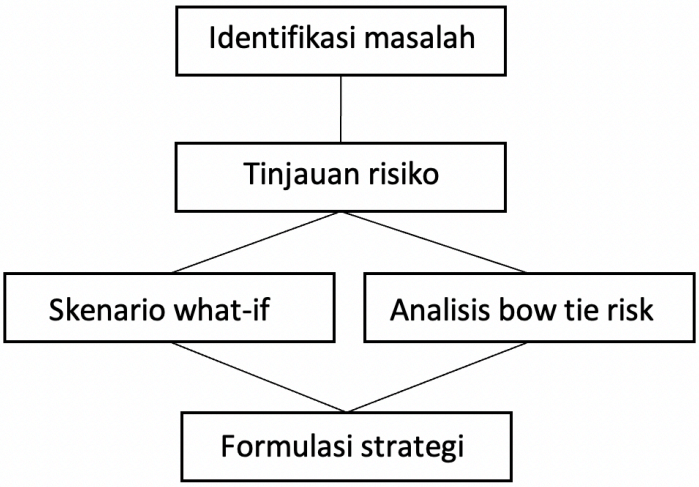
Serangan jenis ini dilakukan dengan memasukkan sebuah konten kedalam situs website yangresmi untuk mempengaruhi pengguna agar memberikan informasi pribadi mereka. Tenik serangan ini dengan memasukkan kode berbahaya pada situs tersebut kemudian pelaku akan mengumpulkan berbagai informasi rahasia didalamnya. Tujuan dari jenis serangan ini yaitu mengambil data informasi rahasia dari komputer pengguna atau komputer pengguna yang dapat dijadikan host untuk menyerang komputer lain.

2.2.6 Phising pada mesin pencari

Manipulasi dari mesin pencari akan menyesatkan korban dengan memberikan izin kepada pelaku untuk memilih domain yang muncul pada situs website phising, walaupun domain tersebut bukan domain yang akan dituju oleh korban. Pelaku jenis serangan ini membuat situs website yang palsu untuk menarik perhatian korban dengan menggunakan beberapa trik seperti diskon, kesempatan, penawaran khusus, peluang kerja, dan lai-lain. Sehingga dari situs website palsu yang dibuat akan digunakan pelaku untuk mencuri identitas atau merusak reputasi perusahaan terkait.

2.3 Kerangka konseptual

Kerangka berpikir merupakan pokok dalam penelitian dimana konsep teoritis akan berubah kedalam definisi operasional yang dapat menggambarkan rangkaian penelitian. Penelitian mengambil beberapa kasus phising pada nasabah bank BRI. Hal ini dilakukan untuk mengidentifikasi masalah bank BRI dan menemukan penyebab terjadinya kasus phising pada nasabah bank BRI sehingga dapat memberikan formula penangan yang tepat.



Berdasarkan kerangka konseptual diatas maka untuk memberikan formula model penanganan yang tepat untuk kasus phising dimulai dengan hal-hal penting sebagai berikut:

1. Identifikasi kasus phising pada nasabah bank BRI dengan melihat modus yag digunakan pelaku, jenis phising, dampak yang ditimbulkan pada nasabah, dan tindak lanjut pihak bank.
2. Peninjauan risiko sejauh mana tingkat risiko yang dialami nasabah berdasarkan hasil dari identifikasi kasus menggunakan analisis matriks risiko. Dari hasil analisis matriks risiko kemudian dilakukan dua analisis yaitu:
   a. Skenario what-if. Analisis yang digunakan untuk memperkirakan perilaku sistem dalam menaggapi kejadian yang tidak terduga.

b. Analisis bowtie risk. Analisis yang menggambarkan peristiwa risiko yang akan dihadapi.

3. Formula penanganan. Setelah melakukan beberapa analisis maka dirumuskan formula penaganan yang tepat berdasarkan tiap jenis kasus.

Kerangka penilitian di atas memandu penelitian dalam menemukan formula yang tepat pada kasus phising nasabah bank BRI dan menghasilkan rencana aksi nyata yang dapat diimplementasikan pada pihak perbankan dalam memberikan penaganan yang dapat meminimalisir risiko phising.

2.4 Identifikasi kasus

Bank BRI merupakan bank yang memiliki nasabah terbanyak di Indonesia. Dengan nasabah yang banyak maka kerentanan untuk terkena risiko dan menjadi sasaran pelaku penyerangan siber khusunya serangan phising. Hal ini dikarenakan jumlah nasabah yang banyak memiliki potensi korban yang lebih banyak karena para pelaku phising akan menargetkan jumlah nasabah yang besar untuk menngkatkan peluang keberhasilan serangan yang dilakukan. Selain itu, dengan jumlah nasabah yang banyak juga mengindikasikan bahwa bank tersebut memiliki sejumlah data yang penting seperti nama, alamat, nomor rekening, nomor kartu kredit yang akan membuat pelaku semakin tertarik melakukan tindakan yang tidak bertangaggungjawab. Terdapat beberapa kasus korban phising yang dialami oleh nasabah bank BRI, antara lain:

Tabel 2. 1 Kasus phising nasabah bank BRI

No	Korban	Modus phishing	Jenis phishing	Tahun kejadian	Dampak yang dialami nasabah	Tindak lanjut dari pihak bank
1	Silvia YAP (52), Malang	Phising dikirim melalui link undangan digital yang dikirim melalui pesan Whatsapp	Social engineering dengan teknik mobile phising	2023	1,4 Miliar	Nasabah tidak mendapatkan kompensasi dari pihak perbankan karena hal ini dinilai terjadi karena kelalaian nasabah. Sehingga dari kejadian ini, bank tidak dapat memberikan ganti rugi sama sekali.
2	Betris, Nunukan.	Phisher mengirim undangan berbentuk APK mengatasnamakan kerbat korban melalui via whatsapp.	Social engineering dengan teknik mobile phising	2023	384 Juta	
3	Irwan Gema (67), Malang	Phisher mengirim undangan berbentuk APK mengatasnamakan kerbat korban melalui via whatsapp.	Social engineering dengan teknik mobile phising	2023	549,4 Juta	

4	Mummad (40), Banjar.	Phisher mengirim undangan berbentuk APK mengatasnamakan kerbat korban melalui via whatsapp.	Social engineering dengan teknik mobile phising	2023	1,5 Miliar	
5	Muhammad Amin, Mamuju.	Phisher mengirim undangan berbentuk APK mengatasnamakan kerbat korban melalui via whatsapp.	Social engineering dengan teknik mobile phising	2023	200 Juta	
6	ST, Padang	Phisher mengatasnamakan pihak bank BRI resmi dengan mengirimkan pesan bahwa adanya perubahan biaya transaksi.	Social engineering phisin dengan unsur content injection-based phising dan domain spoofing.	2022	1,1 Miliar	Nasabah tidak mendapatkan kompensasi dari pihak perbankan karena hal ini dinilai terjadi karena kelalaian nasabah. Sehingga dari kejadian ini, bank tidak dapat memberikan ganti rugi sama sekali.
7	SA, Padang.	Perubahan biaya tarif transfer dengan domain website www.tarif-layanan-bri.com	Social engineering phising dengan unsur content injection-based phising dan domain spoofing.	2022	469 Juta	
8	Fatima, Pontianak.	Melalui via telepon yang mengaku dari BRI pusat, Jakarta dengan modus adanya kenaikan tarif biaya transfer lalu mengirim domain phishing melalu via Whatsapp.	Social engineering phising dengan elemen Vishing (Voice Phishing) dan content injection-based phising	2022	144 Juta	
9	Zainuddin (49), Jomban.	Phisher mengaku dari pihak Bank BRI.	Social engineering phising dengan elemen Vishing (Voice Phishing) dan content injection-based phising	2020	44 Juta	
10	Lily Angel	Phisher mengatasnamakan *costumer service* bank BRI resmi dengan mengirimkan pesan bahwa adanya perubahan biaya transaksi.	Social engineering phising dengan elemen Vishing (Voice Phishing) dan content injection-based phising	2021	9 Juta	

11	Suhartoyo (58), Mojokerto.	Phisher mengaku dari pihak Bank BRI.	Social engineering phising dengan elemen Vishing (Voice Phishing) dan content injection-based phising	2019	67 Juta	

Sumber: Data diolah peneliti, 2023

Dari tabel 2.1 kasus yang terjadi tahun 2019 pada Suhartoyo (58), Mojokerto yang mengalami kerugian sebesar 67 juta akibat phising. Modus pelaku phising melalui via telefon dengan mengatasnamakan pihak bank BRI dengan suara yang khas mirip dengan *costumer service* BRI yang memberikan penyampaian kepada korban bahwa adanya perubahan biaya tarif transfer lalu pelaku mengirimkan link phising kepada korban melalui via SMS. Dari link phising tersebut, korban kemudian diarahkan ke website dengan tampilan yang sangat mirip dengan aplikasi mobile banking BRIMO yang asli, mulai dari design, logo, dan domain yang diberikan. Sehingga, korban tidak merasa curiga dari link phising tersebut. Hingga pada akhirnya, korban mengetik username dan password untuk login ke link tersebut. Ketika korban mengecek saldo di rekeningnya saldonya telah hilang tanpa kode OTP. Korban kemudian melaporkan kejadian tersebut kepada pihak bank BRI setempat. Akan tetapi, ketika korban melapor ke pihak bank BRI, bank BRI meminta untuk menunggu 1 bulan untuk laporan tersebut ditanggapi. 1 bulan kemudian, laporan tersebut tidak kunjung ditanggapi oleh pihak bank BRI setempat. Dari kasus phising tersebut dapat dikategorkan dalam tipe *social engineering phishing* dengan elemen *Vishing (Voice Phishing)* dan *content injection-based phishing.* Hal yang sama juga terjadi pada pada Zainuddin (49), Jombang tahun 2020 dengan total kerugian sebanyak 44 juta,

Kejadian ini juga terjadi pada pasangan suami istri di Padang di tahun 2022. Korban mendapatkan sebuah panggilan suara yang mengatasnamakan pihak bank BRI bahwa terjadi perubahan biaya tarif dari Rp. 6.500 per transaksi menjadi Rp. 150.000 perbulan. Karena korban sering melakukan transaski, maka korba tertarik dengan penawaran tersebut. Dari penawaran yang dilakukan oleh pelaku, pelaku kemudian mengirimkan sebuah tautan yang dikirim via SMS yang berisi

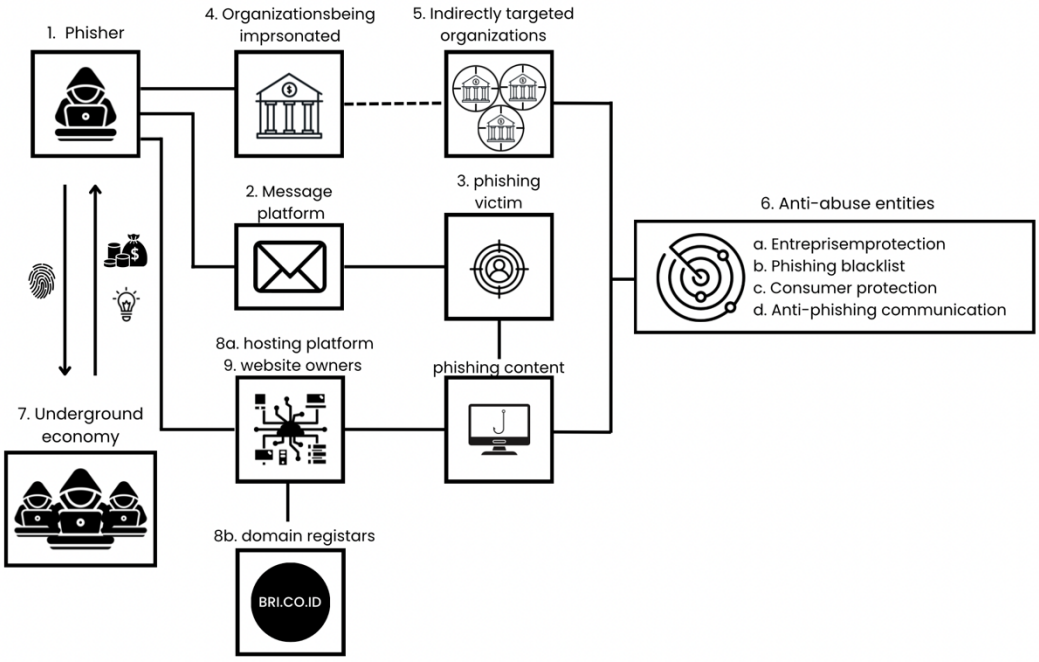
bahwa korban menyetujui hal tersebut dan link tersebut menyuruh korban untuk mengisi username dan password. Setelah mengisi link tersebut, korban mendapatkan pembritahuan mengenai kode OTP. Selang beberapa menit, saldo yang ada direkening milik korban hilang seketika sebesar 1,1 Miliar rupiah. Dari kejadian ini, pihak bank BRI menolak untuk mengganti rugi karena hal ini dinilai akibat kelalaian nasabah. Jenis phising yang digunakan dalam kejadian ini yaitu jenis *social engineering phishing* dengan elemen *Vishing (Voice Phishing)* dan *content injection-based phishing* karena pelaku menggunakan rekayasa sosial dengan berpura-pura sebagai pihak resmi bank BRI kemudian membuat website yang sangat mirip dengan aplikasi resmi BRIMO lalu mengirimkannya ke korban melalui tautan. Hal serupa juga terjadi di tahun yang sama pada SA, Padang dengan total kerugian sebesar 469 Juta dengan jenis phising *social engineering phishing* dengan unsur *content injection-based phishing* dan *domain spoofing* www.tarif-layanan-bri.com; Fatima, Pontianak dengan kerugian sebesar 144 juta. Kasus serupa juga terjadi pada Silvia YAP (52), Malang tahun 2023 merupakan seorang nasabah prioritas bank BRI yang mengalami kerugian sebesar 1,4 Miliar akibat mengklik sebuah tautan phishing. Berbeda dengan modus pelaku sebelumnya, modus pelaku pada kasus ini yaitu mengaku sebagai kerabat terdekat korban dan mengirimkan sebuah undangan digital berbentuk file APK yang didalam file tersebut berisi *malware* yang berbahya. Virus *malware* tersebut dapat mencuri data dari jarak jauh termasuk data *internet banking* yang ada di handphone. Ketika korban mengklik file undangan yang berisi malware tersebut, tanpa disadari saldo yang direkening hilling. Korban baru menyadari hal tersebut ketika terdapat pemberitahuan saldo keluar yang tidak ia lakukan sama sekali. Dari kejadian tersebut korban melaporkan ke pihak bank tetapi pihak tidak dapat memberi ganti rugi dari kejadian tersebut dan melapor ke OJK terkait layanan keamanan yang tidak maksimal kepada nasabah priorotas. Selain Silvia, kasus di tahun yang sama juga terjadi pada Irwan Gema (67), Malang yang mengalami kerugian 549,4 Juta; Betris, Nunukan. Denan kerugian sebesar 384 Juta; Muhammad (40), Banjar dengan kerugian sebesar 1,5 Miliar; Muhammad Amin,

Mamuju dengan kerugian sebesar 200 Juta; dengan modus yang sama yaitu mengirimkan undangan digital yang berbentuk APK yang berisi *malware.*

Berdasarkan kasus diatas mengindikasikan bahwa serangan phising pada nasabah bank BRI masih sering terjadi. Faktor utama penyebab terjadinya phising pada nasabah yaitu ketidaktahuan dan kelalaian nasabah atau pengguana. Selain itu ketertarikan nasabah untuk mendapatkan informasi berupa memberikan tawaran perubahan biaya transfer yang lebih murah dibanding biaya transfer sebelumnya, sehingga hal ini memicu nasabah merasa tertarik untuk membuka link tersebut. Disisi lain modus pelaku yang semakin canggih dan terkini membuat korban lebih sulit untuk membedakan antara tautan asli dan tautan berbahaya. Modus terkini yang digunakan para pelaku phising pada kasus diatas yaitu mengirimkan file menyerupai undangan digital, namun file tersebut merupakan file berisi apk yang sudah terinfeksi virus malware sehingga dapat menyebabkan saldo nasabah menjadi berkurang bahkan habis.

Adapun gambaran alur terjadinya phising yang dialami nasabah dapat dilihat pada gambar dibawah ini:

Gambar 2. 1 Phishing ecosystem



Sumber: Oest, IEEE, 2019

Gambar diatas menjelaskan alur proses serangan phishing yang digambarkan dalam sebuah ekosistem phishing. Tahap pertama proses terjadinya serangan phising yaitu dimulai oleh pelaku serangan phishing mengumpulkan informasi data mengenai target yang akan menjadi korban serangan phising. Informasi data tersebut dikumpulkan melalui beberapa metode yaitu dengan membuat situs website palsu yang sangat mirip dengan situs wesite resmi perusahaan, membeli informasi dark web, dan melalui pesan teks atau media sosial yang telah dikumpulkan. Setelah menargetkan korban, langkah selanjutnya yang dilakukan yaitu mengirimkan dan menyebarkan link situs website palsu dan virus phising melalui media sosial dan pesan teks, seperti email, whatsapp, dan lain-lain. Para phisher akan mencari cara untuk meyakinkan korban dengan berpura-pura sebagai organisasi resmi dengan tampilan visual yang sama persis, logo, serta gaya bahasa yang sangat mirip dengan layanan resmi sebuah organisasi. Sehingga, ketika korban percaya bahwa itu berasal dari organisasi yang resmi maka dana yang dimiliki akan hilang.

Gambar 2. 2 Contoh phising

PT. BANK RAKYAT INDONESIA (PERSERO)Tbk
KANTOR PUSAT JAKARTA SELATAN
Jl. Jenderal Sudirman Kap.44-46 Tlp. (021)879857

BANK BRI

Nomor : 0311 / BRI./VI / 2022
Perihal : Perubahan Tarif Transfer Bank Lain
Lampiran : -

Kepada.
Yth.Bapak/Ibu
Nasabah Bank BRI

Dengan Hormat.
Sehubungan Dengan Meningkatkan Kualitas dan Kenyamanan Nasabah Bertransaksi.
Mulai Nanti Malam Pergantian Hari Dan Pergantian Tanggal, Pihak Bank Bri
Mengubah Tarif Transfer Bank lain: Rp 6.500 IDR Per Transaksi, Di Ubah Menjadi,
Tarif: 150.000 perbulan.(auto debit dari rekening Tabungan) Unlimited Transaksi

1. Apakah Setuju Dengan Tarif Baru 150.000 Perbulan Unlimited Transaksi.
2. Tidak Setujuh Dan Mau Tetap ke Tarif Yang Lama 6.500 per Transaksi

Jika Bapak/Ibu Tidak ada Konfirmasi, Berarti Di Anggap Setujuh Dengan Tarif Yang
Baru Untuk Perubahan Skema Tarif Dalam Tahap Percobaan Untuk 6 bulan Kedepan.
Dengan Ini Di Pertanyakan Kepada Bapak/Ibu Nasabah Bank BRI, Jika Tidak Setujuh
Dengan Tarif Yang Baru Silahkan Mengisi formulir Yang Di kirim.

N.B
Jika Bapak/Ibu tidak Ada KONFIRMASI maka di Anggap SETUJUH. Untuk
penagihan setiap bulannya Rp.150.000 dari rekening Tabungan BRI nya
Adanya transaksi atau tidak tetap akan di Potong.

PT Bank Rakyat Indonesia (persero) Tbk

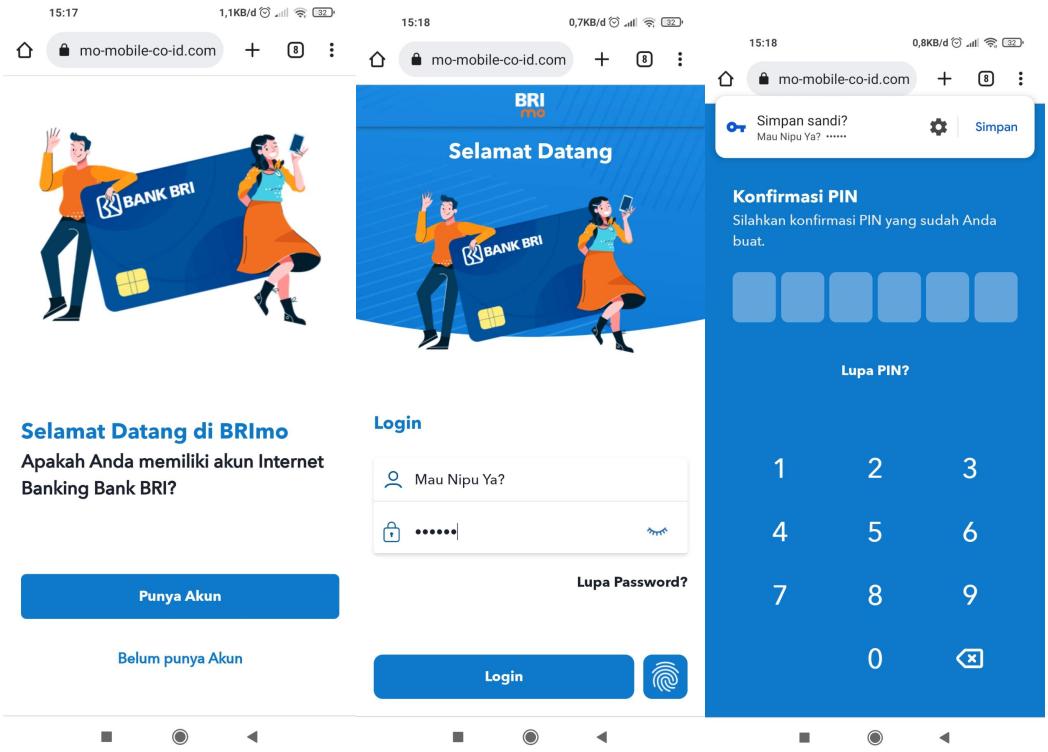
SUNARSO
Direktur BANK BRI

e-Pay BRI BRILink

Sumber: Twitter, 2023

Gambar 2.2 merupakan contoh gambar phising yang disebarkan oleh phisher kepada beberapa nasabah bank BRI. Teknik yang digunkan yaitu berpura-pura sebagai pihak resmi bank BRI lalu menginfokan kepada korban bahwa adanya perubahan biaya tarif transefer. Dari gambar 2.2 diatas dapat kita lihat bahwa phisher menggunakan element grafis yang sama, merk dagang, logo, dan tampilan yang sangat persis dari Bank BRI secara resmi. Setelah memberikan pemberitahuan tersebut kepada korban, maka pelaku akan mengirimkan sebuah link phising (htpss://brimo.ganti-tarif.com) yang akan tertuju pada sebuah layanan aplikasi mobile banking BRI.

Gambar 2. 3 BRIMO phising



Sumber: Twitter, 2023

Gambar 2.3 merupakan tampilan aplikasi bank BRIMO yang telah dikirim oleh phisher. Tampilan BRIMO yang telah dibuat oleh phiser sangat mirip dengan tampilan BRIMO yang resmi dengan visual design dan logo yang digunakan. Jika korban memasukkan pin asli maka korban akan kehilangan uang yang dimiliki dari aplikasi BRIMO resmi.

Ketika pesan mengandung phising tidak buka dan tidak ditanggapi oleh calon korban, maka serangan siber seperti malware tidak akan menginfeksi pada smartphone korban sehingga tidak akan menimbulkan kerugian. Dalam konteks ini, pengetahuan terkait bahaya phising sangat penting dalam membantu dan mencegah terjadinya serangan phising. Oleh karena itu, edukasi terkait cara identifikasi website berbahaya sangat diperlukan khususnya bagi nasabah genarasi X dan boomer. Genarasi X dan boomer menjadi fokus utama dalam

mencegah terjadinya phising, mengingat generasi tersebut sering menjadi sasaran phisher dan dari beberapa kasus phising banyak terjadi pada generasi tersebut. Hal ini dikarenakan korban tidak dapat membedakan website resmi dan website palsu karena secra tampilan yang sangat mirip dengan website resmi.

2.5 Analisis internal phising

Analisis intenal mengenai kondisi dan kelemahan internal dapat membantu dalam merancang model penanganan phising yang tepat dan terintegrasi. Untuk melakukan analisis ini maka dapat dilakukan dengan megngidentifikasi kerentanan internal yang mungkin dapat dimanfaatkan oleh pelaku serangan phising. Sehingga identifikasi tersebut sebagai berikut:

a. Sistem keamanan dan infrastruktur internal bank BRI

   Dalam mengevaluasi keamanan perangkat keras dan perangkat lunak, BRI telah mengadopsi kebijakan keamanan teknologi informasi yang mengacu pada standar internasional seperi ISO/IEC 270001:2013 dan PCI DSS. Hal ini menunjukkan adanya upaya perusahaan dalam pengamanan teknolgi informasi. Dalam implementasinya, kebijakan keamanan internal bank BRI telah disusun berdasarkan regulasi ekternal dan standar industri yang tercermin pada IT security policy dan prosedur internal lainnya.

b. Pelatihan dan kesadaran karyawan

   Pelatihan dan kesadaran risiko sangat penting dalam keberlangsungan perusahaan. Hal ini dikarenakan terdapat korelasi yang kuat antara pendidikan karyawan dan keamanan teknis. Karena memeberikan pelatihan karywan untuk mengenasi risiko dapat menjadi pertahanan terbaik bagi perusahaan. Dalam hal ini, bank BRI telah menerapkan program peningkatan kesadaran melalui e-learning, webinar, dan kampanye email phishing. Program seperti kampanye email phising dapat membantu kesadaran karywan terhadap ancaman phising.

c. Teknologi

   Dalam melakukan monitoring *cyber threat,* bank BRI memiliki bagian khusus yaitu *security operation center* (SOC). Pada bagian SOC bank BRI melakukan

monitoring terhadap ancaman siber secara kontinu. Dalam melakukan monitoring keamanan siber, bank BRI juga melakukan secara proaktif melalui layanan threat hunting dan threat intelligence service yang dikembangkan oleh provider berskala internasional.

d. Manajemen risiko internal

Pada proses manajemen risiko internal perusahaan, bank BRI mengadopsi prosedur manajemen risiko yang mengacu pada regulasi seperti Peraturan Otoritas Jasa Keuangan No. 38/POJK.03/2016 Tentang Penerapan Manajemen risiko Dalam Penggunaan Teknologi Informasi Oleh Bank Umum.

Berdasarkan poin-poin diatas menunjukkan bahwa bank BRI telah melakukan upaya dalam menciptakan lingkungan yang kuat terhadap ancaman keamanan siber dengan menerapkan strategi keamanan informasi yang komprehensif, mengintegrasikan regulasi dengan kebijakan internal, memberikan pelatihan dan kesadaran pada karyawan. Akan tetapi, meskipun telah menerapkan beberapa startegi terdapat beberapa kelemahan yang dapat menjadi celah bagi pelaku sehingga masing sering terjadi serangan phising pada nasabah yang menyebabkan kerugian.

2.6 Analisis matriks risiko

Matriks risiko merupakan tabel dengan kategori probabilitas pada satu sumbu dan dampak pada sumbu yang lain. Menurut Davidsson (2003), matriks risiko dapat digunakan dalam mengurutkan tingkat risiko. Probabiltas dan dampak diestimasi dan dalam kategori yang berbeda dan ditujukan dalam matriks risiko. Hussey (1978) juga menjelaskan bahwa matriks risiko merupakan alat bantu dua dimensi dalam pengambilan keputusan. Pembuatan matriks risiko dimulai dari proses identifikasi masalah, kemudian diberikan bobot penilaian berdasarkan skala probabilitas dan dampak yang digunakan. Adapun skala penilaian risiko yang digunakan untuk menggambarkan probabilitas dan dampak yaitu:

1. Skala probabilitas

Tabel 2. 2 Skala probabilitas matriks risiko

Tingkat	Deskripsi	Keterangan

1	Sangat rendah	Hampir tidak pernah, sangat jarang terjadi
2	Rendah	Jarang terjadi
3	Sedang	Dapat terjadi sekali-kali
4	Tinggi	Sering terjadi
5	Sangat tinggi	Sangat sering terjadi

2. Skala dampak

Tabel 2. 3 Skala dampak matriks risiko

Tingkat	Deskripsi	Keterangan
1	Sangat rendah	Hampir tidak pernah, sangat jarang terjadi
2	Rendah	Jarang terjadi
3	Sedang	Dapat terjadi sekali-kali
4	Tinggi	Sering terjadi
5	Sangat tinggi	Sangat sering terjadi

2.7 Analisis skenario

Analisis skenario merupakan analisis yang digunakan untuk memperkirakan perilaku sistem dalam menaggapi kejadian yang tidak terduga. Selain itu, analisis ini juga dapat digunakan untuk mengeksplorasi perumahaan dalam kinerja sistem. Probabilitas kejadian dan kemungkinan dampak dari sebuah skenario harus dipertimbangkan secara bersamaan untuk mengembangkan sebuah rencana strategis berdasarkan hasil analisis skenario. Adapun pendekatan yang dapat digunakan dalam analisis skenario yaitu dengan pendekatan skenario *what-if.* Skenario *What-if* merupakan sebuah analisis kuantitatif dengan pendekatan kualitatif untuk mengentahui kemungkinan yang akan terjadi dari suatu masalah yang ada. Analisis *what-if* juga merupakan sebuah model yang bertujuan untuk menjawab pertanyaan “apa yang terjadi pada keluaran jika terdapat perubahan pada masukan”. Jika perubahan dimasukkan tidak teralu signifikan, maka hal ini dapat disebut sebagai analisis sensivitas. Karena analisis sensivitas menilai seberapa sensitifnya keluaran terhadap perubahan kecil terjadi di parameter penentu keluaran.

2.8 Analisis bow tie risk

Analisis bow tie risk merupakan sebuah metode yang disajikan dalam bentuk diagram berbentuk dasi kupu-kupu yang menggambarkan peristiwa risiko yang akan dihadapi. Pendekatan analisis bow tie menyajikan visualisasi hubungan antara masalah utama, penyebab, pencegahan dan penanganan. Teknik analisis ini memiliki beberapa bagian yang saling terhubung dalam menjelaskan sebuah kejadian risiko dengan penyebab dan konsekuensi, serta menggambarkan bagaimana peristiw risiko dapat ditangani, antara lain:

1. Bahaya (Hazard)

   Langkah awal dalam membuat analisis bow tie risk yaitu menentukan suatu bahaya, baik dari dalam, di sekitar, atau bagian dari organisasi yang memiliki potensi menyebabkan kerusakan atau kerugian. Hal tang terpenting pada bagaian ini yaitu menemukan hal-hal/peristiwa organisasi yang dapat menyebabkan dampak negative jika tidak dilakukan penanganan.

2. Peristiwa puncak (Top Event)

   Setelah bahaya teridentifkasi, maka langkah selanjutnya yaitu menentukan peristiwa puncak yang mungkin terjadi. Peristiwa puncak merupakan keadaan atau situasi ketika penanganan terhadap bahaya tidak ada. Dengan kata lai, peristiwa puncak dipilih sebelum memberikan dampak yang actual.

3. Penyebab (cause)

   Penyebab merupakan segala sesuatu yang dapat menyebabkan peristiwa puncak terjadi.

4. Konsekuensi (consequence)

   Konsekuensi yaitu dampak negative yang timbul akibat peristowa puncak.

5. Pencegahan

   Kontrol pencegahan ini berfungsi untuk menangguhkan atau menahan agar penyebab tidak terjadi, dan jika sampai terjadi tidak menimbulkan dampak yang besar sehingga dapat dikendalikan.

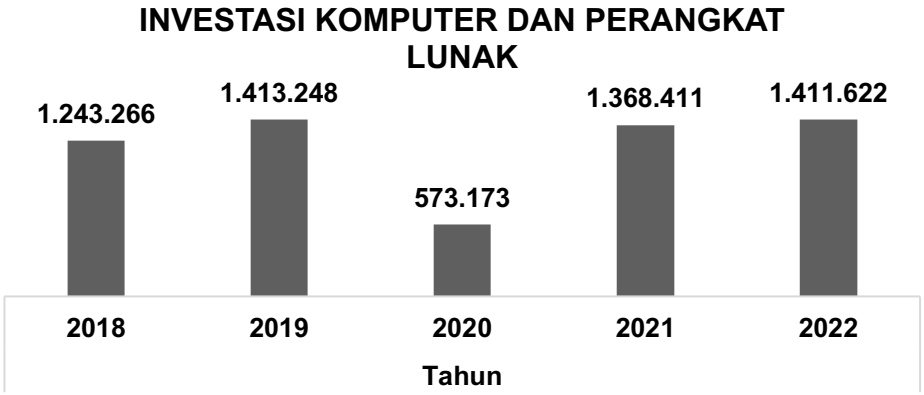
6. Mitigasi

   Control mitigasi ini dibuat untuk memastikan bahwa jika peristiwa puncak terjadi, skenario dari konsekuensi yang telah dibuat tidak mengalami

peningkatan sehingga menjadi konsekuansi actual dan/atau untuk meminimalisir konsekuensi yang akan telah terjadi.

2.9 Kondisi keuangan perusahaan

Analisis laporan keuangan merupakan suatu poroses dalam rangka menganalisis atau mengevaluasi keadaan keuangan perusahaan, hasil-hasil operasi perusahaan masa lalu dan masa depan. Laporan keuangan ini berfungsi sebagai alat informasi yang untuk mengevaluasi kekuatan dan kelemahan perusahaan yang tercermin pada laporan keuangan. Dalam penelitian ini, analisis laporan keuangan dilakukan untuk menilai kemampuan perusahaan dalam mengahadapi tantangan keamanan teknologi informasi dengan melihat beberapa aspek yaitu investasi komputer dan perangkat lunak, beban operasional, dan ATMR untuk risiko operasional. Invetasi barang modal khususnya dalam komputer dan perangkat lunak menunjukkan kesiapan perusahaan dalam menghadapi tantangan keamanan teknologi informasi. Selain itu, beban operasional juga menjadi hal yang diperhatikan khususnya pada beban opersioanal komputer dan perangkat lunak, penelitian dan pengembangan produk, dan pendidikan dan pelatihan karyawana. Beban operasional yang dilakukan oleh perusahaaan menggambarkan bagaimana perusahaan memberikan upaya dalam meningkatkan pemahaman kepada karyawan mengenai literasi keamanan teknologi informasi sehingga dapat mengmbangkan solusi inovatif. Gambar 2. 4 Investasi komputer dan perangkat lunak Bank BRI



Sumber: Data Sekunder diolah Annual Report BRI, 2023

Gambar 2.4 merupakan investasi barang modal yang dilakukan bank BRI 5 tahun terkahir. Dari diagram diatas dapat diketahui bahwa terjadi fluktuasi investasi barang modal yang dilakukan bank BRI. Pada tahun 2018-2019 terjadi pertumbuhan dari 1,2 Miliar menjadi 1,4 Miliar yang jika di persentasekan sebesar 13.67%. Hal ini mencerminkan bahwa adanya pertumbuhan ekonomi yang positif, kepercayaan bisnis, sehingga berdampak pada pertumbuhan nilai invesasti dalam teknologi. Pada tahun 2019-2020 terjadi penurunan yang sangat drastis dengan persentase sebesar 59,51%. Berdasarkan laporan keuangan, hal ini terjadi adanya fenomena Covid 19 sehingga menyebabkan pertumbuhan ekonomi yang negative pada kuartal II tahun 2020. Penurunan investasi yang terjadi menggambarkan bahwa adanya penundaan proyek dan penghematan biaya yang dilakukan oleh perusahaan sebagai respons terhadap ketidakpastian ekonomi yang disebabkan oleh pandemi. Tahun 2020-2022 terjadi lonjakan drastic dibanding tahun tahun sebelumnya. Hal ini dikarenakan pada tahun 2021 terjadi pemulihan ekonomi yang mempengaruhi keputusan investasi perusahaan. Sehingga, permintaan dan kinerja yang meningkat akan mendorong investasi salah satunya pada bidang teknologi informasi.

Tabel 2. 4 Beban operasional Bank BRI

BEBAN OPERASIONAL	Tahun				
	2018	2019	2020	2021	2022
Komputer dan perangkat lunak	54.453	41.042	74.721	67.782	82.586
Pendidikan dan pelatihan karyawan	633.758	724.583	365.787	434.207	1.153.346
Penelitian dan pengembangan produk	24.105	29.715	23.670	365.317	279.262

Sumber: Annual Report BRI diolah, 2023

Tabel 2.1 merupakan nilai dari beban operasional yang dikeluarkan oleh bank bank BRI pada 5 tahun terkahir. Dari tabel diata mengintrepretasikan bahwa terjadi fluktuasi dari tahun ke tahun. Pada tahun 2018-2019, beban operasional pada computer dan perangkat lunak terjadi penurunan sebesar 24,63%. Hal ini dikarenakan perusahaan melaukan efesiensi operasional. Jika dikaitkan dengan investasi barang modal pada computer dan perangkat lunak pada gambar 2.4 mengindikasikan bahwa terjadi peningkatan investasi dan penurunan beban operasional pada computer dan perangkat lunak di tahun yang sama. Hal ini menandakan bahwa secara prinsip umum ekonomi menandakan bahwa pengelolaan sumber daya dilakukan secra efisien sehingga memberikan hubungan yang positif dalam pengembangan yang dilakukan bank BRI. Ini juga tercermin pada beban operasional pada pendidikan dan pelatihan karyawan; penelitian dan pengembangan produk yang mengalami peningkatan di tahun yang sama. Ini mengindikasikan bahwa perusahaan terus melakukan upaya pengembangan perusahaan melalui peningkatan literasi dan kemampuan karyawan.