

Analisis Pengaruh Sistem Keamanan Informasi Perbankan pada Nasabah Pengguna Internet Banking BRI

Reynaldi Kurniawan¹, Tigar Riski Septiono², Dwi Ananda Rizki Saputra^{3*}

¹ Teknik Informatika
Tegalondo, Wonosari, Klaten, Jawa Tengah

¹kurniawanreynaldi8@gmail.com

² Teknik Informatika
Klaruan Rt.03 Rw.16 palur, Mojolaban Sukoharjo, Jawa Tengah

²riskiseptiono0@gmail.com

³ Teknik Informatika
Ngasinan, PagerGunung RT 03 RW 01, Sukoharjo, Jawa Tengah

³rizkibarker15@gmail.com
(penulis korespondensi)

Abstrak— Industri perbankan telah berkembang pesat dalam adopsi teknologi dan informasi terbaru, terutama dengan meningkatkan layanan perbankan elektronik seperti internet banking. Dalam menciptakan layanan perbankan yang terpercaya bagi pelanggan, menjaga keamanan sistem informasi yang berkaitan dengan transaksi perbankan, khususnya yang berkaitan dengan layanan perbankan online, menjadi fokus utama. Hasil analisis menunjukkan bahwa perlindungan data konsumen dan keamanan transaksi merupakan bagian penting dari keberhasilan perbankan elektronik. Hasil analisis dilakukan dengan mengidentifikasi manfaat dan tantangan dalam melaksanakan perbankan elektronik, mengevaluasi tata kelola keamanan informasi, dan memahami regulasi terkait perlindungan data konsumen serta tata kelola risiko operasional. Untuk menghadapi ancaman keamanan informasi yang semakin kompleks di era digital, sangat penting untuk meningkatkan tata kelola keamanan informasi, menggunakan teknologi keamanan terbaru, dan memberikan pelatihan berkelanjutan bagi karyawan perbankan. Diharapkan bahwa analisis ini akan memberikan pemahaman mendalam tentang tantangan dan peluang dalam menerapkan layanan perbankan elektronik serta menekankan bahwa keamanan informasi sangat penting untuk mendukung kemajuan industri perbankan di era digital.

Kata Kunci: Perbankan Elektronik, Internet Banking, Keamanan Informasi, Teknologi, Nasabah

Abstract—The banking industry has rapidly evolved in adopting the latest technology and information, especially by enhancing electronic banking services such as internet banking. In creating trustworthy banking services for customers, ensuring the security of information systems related to banking transactions, especially those related to online banking services, becomes a primary focus. The analysis indicates that protecting consumer data and transaction security are crucial parts of the success of electronic banking. The analysis is conducted by identifying the benefits and challenges of implementing electronic banking, evaluating information security governance, and understanding regulations related to consumer data protection and operational risk management. To address increasingly complex information security threats in the digital age, it is crucial to enhance information security governance, utilize the latest security technology, and provide ongoing training for banking staff. It is expected that this analysis will provide a deep understanding of the challenges and opportunities in implementing electronic banking services and emphasize that information security is vital to support the advancement of the banking industry in the digital era.

Keywords: Electronic Banking, Internet Banking, Information Security, Technology, Customers

I. PENDAHULUAN

Bank Rakyat Indonesia (BRI) didirikan pada tanggal 16 Desember 1895 di Purwokerto, Jawa Tengah oleh Raden Bei Aria Wirjaatmadja. BRI awalnya bernama De Poerwokertosche Hulp en Spaarbank der Inlandsche Hoofden yang bertujuan untuk melayani masyarakat pribumi terutama dalam hal simpan pinjam. Dalam perkembangannya, BRI telah mengalami berbagai perubahan nama dan bentuk badan hukum hingga menjadi salah satu bank terbesar di Indonesia.

Masa Kemerdekaan dan Nasionalisasi
Setelah Indonesia merdeka, BRI dinasionalisasi pada tahun 1946 dan menjadi Bank Negara Indonesia Unit

Pada tahun 1960, BRI ditetapkan sebagai bank umum milik negara dan kembali menggunakan nama Bank Rakyat Indonesia.

Peran dalam Pembangunan Ekonomi
BRI memainkan peran penting dalam pembangunan ekonomi Indonesia, terutama dalam sektor pertanian dan usaha mikro, kecil, dan menengah (UMKM). BRI menjadi pelopor dalam penyaluran kredit usaha kecil melalui program Kredit Usaha Rakyat (KUR) yang dimulai pada tahun 2007. Program ini membantu meningkatkan akses permodalan bagi pengusaha kecil dan mikro di seluruh Indonesia.

Transformasi Digital

Dalam beberapa dekade terakhir, BRI telah melakukan transformasi digital yang signifikan. Bank ini mengembangkan berbagai layanan perbankan digital untuk memudahkan nasabah dalam melakukan transaksi. Layanan-layanan tersebut meliputi internet banking, mobile banking, dan BRILink (agen banking) yang memungkinkan masyarakat di daerah terpencil untuk mengakses layanan perbankan.

Ekspansi dan Modernisasi

BRI terus melakukan ekspansi jaringan dengan membuka kantor cabang dan unit layanan di seluruh Indonesia, bahkan hingga ke daerah-daerah terpencil. Modernisasi sistem perbankan juga terus dilakukan untuk meningkatkan efisiensi dan kualitas layanan. Pada tahun 2018, BRI memperkenalkan satelit BRIsat, yang merupakan satelit pertama yang dimiliki oleh bank di dunia, untuk mendukung jaringan komunikasi yang lebih andal.

Kinerja dan Prestasi

BRI telah mendapatkan berbagai penghargaan atas kinerjanya yang unggul. Bank ini dikenal sebagai bank dengan kinerja keuangan yang stabil dan terus tumbuh dari tahun ke tahun. BRI juga dikenal sebagai bank dengan kontribusi besar dalam pembiayaan sektor UMKM di Indonesia. Hingga kini, BRI tetap menjadi bank terbesar di Indonesia dari segi aset, jumlah nasabah, dan jaringan layanan.

Tanggung Jawab Sosial

Selain fokus pada bisnis, **BRI** juga aktif dalam menjalankan program tanggung jawab sosial perusahaan (CSR). Program CSR BRI meliputi bidang pendidikan, kesehatan, lingkungan, dan pemberdayaan masyarakat. Melalui berbagai inisiatif sosial, BRI berusaha untuk memberikan kontribusi positif bagi masyarakat dan lingkungan.

Kesimpulan

BRI telah melalui perjalanan panjang sejak didirikan pada tahun 1895 hingga menjadi salah satu bank terbesar di Indonesia. Dengan komitmen untuk terus berinovasi dan memberikan layanan terbaik, BRI memainkan peran kunci dalam pembangunan

ekonomi dan kesejahteraan masyarakat Indonesia. Transformasi digital dan ekspansi jaringan yang dilakukan BRI menunjukkan bahwa bank ini siap menghadapi tantangan di masa depan dan terus berkontribusi dalam memajukan perekonomian nasional.

Maksud Dan Tujuan Riset

Tujuan dari penelitian ini adalah untuk melihat bagaimana sistem keamanan informasi perbankan berdampak pada nasabah yang menggunakan internet banking BRI. Dengan demikian, penelitian ini diharapkan dapat menambah pengetahuan tentang bagaimana sistem keamanan informasi perbankan dapat meningkatkan keamanan transaksi nasabah dan mengurangi risiko keamanan yang terkait dengan menggunakan internet banking.

II. METODOLOGI PENELITIAN

Penelitian ini menggunakan data sekunder dari berbagai sumber referensi, termasuk buku, arsip, majalah, artikel, dan dokumen terkait. Metode pengumpulan data ini memungkinkan peneliti untuk menemukan data yang relevan untuk mendukung analisis dampak sistem keamanan informasi perbankan terhadap pelanggan BRI yang menggunakan layanan internet banking. Tahapan penelitian ini dimulai dengan menentukan topik penelitian dan ruang lingkup penelitian, kemudian dilanjutkan dengan mencari sumber data yang relevan melalui studi literatur. Data yang dikumpulkan kemudian disusun, dianalisis, dan dievaluasi untuk mendukung analisis dampak sistem keamanan informasi perbankan terhadap pelanggan BRI. Oleh karena itu, penelitian ini meningkatkan pemahaman kita tentang cara BRI melindungi data dan transaksi nasabahnya melalui penerapan sistem keamanan informasi yang kuat dan canggih.

Penelitian ini melibatkan seluruh nasabah Bank Rakyat Indonesia di Kabupaten Mamuju. Metode pengumpulan data kuantitatif digunakan, dengan sampling tidak sengaja digunakan. 40 responden dipilih berdasarkan kriteria bahwa mereka adalah nasabah BRI Kabupaten Mamuju yang menggunakan dan memahami mobile banking. Kuesioner ini dibuat untuk tujuan mendapatkan data primer, sedangkan data sekunder diperoleh melalui

studi dokumentasi untuk membuat rumusan masalah, tinjauan pustaka, dan hipotesis, dan wawancara dengan klien atau narasumber yang menggunakan mobile banking.

Uji validitas dilakukan untuk mengevaluasi keakuratan dan kecermatan instrumen atau alat ukur yang digunakan pada variabel penelitian. rtabel digunakan untuk melakukan kriteria pengujian signifikan, di mana item dapat dinyatakan valid jika $r_{hitung} \geq r_{tabel}$. Uji realibilitas digunakan untuk mengetahui apakah instrumen pengumpulan data dapat diandalkan dan menghasilkan data yang konsisten dengan fakta.

Suatu alat ukur dianggap reliabel jika nilai Cronbach Alpha lebih dari 0,60. Analisis data dalam penelitian ini dilakukan dengan menggunakan analisis regresi linier berganda yang diproses menggunakan program SPSS. Selain itu, model hipotesis diuji secara parsial dan simultan.

Regresi linier berganda menghasilkan rumus berikut: $Y = a + b_1X_1 + b_2X_2 + b_3X_3 + e$

III. HASIL DAN PEMBAHASAN

Faktor kemudahan, keamanan, resiko, dan kepuasan pelanggan adalah variabel penelitian yang digunakan dalam penilaian validitas dan realibilitas. Berdasarkan hasil pengolahan data dengan program SPSS, semua pernyataan valid karena tabel korelasi harus menunjukkan angka setidaknya 0,312. Selain itu, hasil realibilitas untuk semua variabel yang dikaji harus memiliki nilai setidaknya 0,60. Hal ini menunjukkan bahwa semua pernyataan yang berkaitan dengan setiap variabel dapat dianggap dapat diandalkan atau dapat dipercaya, sehingga alat penelitian ini layak untuk digunakan.

Penelitian ini bertujuan untuk mengetahui pengaruh atau keeratan hubungan masing-masing variabel. Tabel berikut menunjukkan hasil analisis regresi linier berganda.

Tabel 1

Hasil Analisis Regresi Linier Berganda

Model		Coefficients ^a				
		Unstandardized Coefficients		Standardized Coefficients		Sig.
		B	Std. Error	Beta	t	
1	(Constant)	-4.685	4.920		-.952	.347
	kemudahan (x1)	.728	.176	.566	4.143	.000
	keamanan (x2)	.423	.164	.326	2.584	.014
	resiko (x3)	-.041	.083	-.049	-.495	.623

a. Dependent Variable: kepuasan (y)

Sumber: Hasil Olah Data SPSS Versi 23, 2022

Perolehan menunjukkan nilai constanta sebesar -4,685 dengan nilai faktor kemudahan 0,728, nilai faktor keamanan 0,423 dan nilai faktor resiko -0,041 maka $Y = -4,685 + 0,728 + 0,423 - 0,041 + e$

Pengaruh faktor kemudahan terhadap kepuasan nasabah dalam menggunakan mobile banking di Kabupaten Mamuju: Faktor kemudahan memiliki t-hitung 4,143 lebih besar dari 2,024 dan nilai signifikan 0,000 lebih kecil dari 0,05. Ini menunjukkan bahwa faktor kemudahan berpengaruh positif dan signifikan terhadap kepuasan nasabah dalam menggunakan mobile banking. Hasil penelitian ini berbeda dengan penelitian Nila Erina (2021:80), yang menemukan bahwa faktor kemudahan tidak memiliki pengaruh signifikan terhadap kepuasan pelanggan.

Perbedaan ini terjadi karena cara pelanggan melihat kemudahan mobile banking berbeda-beda di setiap daerah.

Menurut pendapat, kemudahan menggunakannya dapat membuat pelanggan merasa senang sehingga mereka ingin menggunakannya lagi dan lagi. Penggunaan berulang akan menyebabkan kepuasan tersendiri karena dianggap dapat membantu kebutuhan masyarakat, terutama dalam hal transaksi. Faktor keamanan memiliki pengaruh positif dan signifikan terhadap kepuasan nasabah dalam menggunakan layanan perbankan mobile di Kabupaten Mamuju, dengan t-hitung 2,584 lebih besar dari 2,024 dan nilai signifikan 0,014 lebih rendah dari 0,05. Hasil penelitian ini sesuai dengan penelitian yang dilakukan oleh Wahyu Jalil Saputro (2020:81), yang menemukan bahwa terdapat pengaruh signifikan antara keamanan dan kepuasan nasabah dalam menggunakan layanan perbankan mobile.

Hal ini menunjukkan bahwa semakin aman teknologi, semakin puas nasabah dengan mobile banking. Saat ini, nasabah dapat melakukan verifikasi untuk setiap transaksi melalui layanan autentifikasi mobile banking untuk melindungi data mereka.

Pengaruh faktor resiko terhadap kepuasan nasabah menggunakan mobile banking di Kabupaten Mamuju: Faktor resiko memiliki t-hitung -0,495 lebih besar dari 2,024 dan t-tabel memiliki nilai

signifikan 0,623 lebih besar dari 0,05. Ini menunjukkan bahwa faktor resiko tidak berdampak signifikan terhadap kepuasan nasabah menggunakan mobile banking di Kabupaten Mamuju. Hasil penelitian ini sesuai dengan penelitian Nurul Mukaromah (2020:66), yang menemukan bahwa faktor resiko tidak memiliki pengaruh yang signifikan terhadap penggunaan mobile banking.

Tabel 2

Hasil Uji Simultan (Uji F)

ANOVA ^a						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	522.063	3	174.021	35.689	.000 ^b
	Residual	175.537	36	4.876		
	Total	697.600	39			

a. Dependent Variable: kepuasan (y)
b. Predictors: (Constant), resiko (x3), keamanan (x2), kemudahan (x1)

Sumber: Hasil Olah Data SPSS Versi 23, 2022

Hasil uji F menunjukkan bahwa nilai yang diperoleh adalah 35,689, sedangkan nilai Ftabel sebesar 2,866. Maka dapat diketahui bahwa nilai Fhitung $35,689 > F$ tabel 2,87 dengan tingkat signifikan

$0,000 < 0,05$, sehingga dapat disimpulkan bahwa variabel kemudahan, keamanan, dan resiko secara bersama-sama berpengaruh signifikan terhadap kepuasan nasabah dalam menggunakan mobile banking di Kabupaten Mamuju, dengan demikian hipotesis dapat diterima.

Tabel 3

Hasil Koefisien Determinasi (R²)

Model Summary				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.865 ^a	.748	.727	2.208

a. Predictors: (Constant), resiko (x3), keamanan (x2), kemudahan (x1)

Sumber: Hasil Olah Data SPSS Versi 23, 2022

Berdasarkan tabel 3 diperoleh nilai koefisien determinasi sebesar 0,748, hal tersebut menunjukkan bahwa sebesar 74,8% variasi kepuasan nasabah dalam menggunakan mobile banking dapat dijelaskan dengan baik oleh faktor kemudahan, keamanan, dan resiko. Dengan kata lain bahwa kontribusi yang diberikan faktor kemudahan, keamanan, dan resiko terhadap kepuasan nasabah Bank

BRI dalam menggunakan mobile banking di Kabupaten Mamuju sebesar 74,8%, sedangkan sisanya sebesar 0,252 atau 25,2% dipengaruhi atau dijelaskan oleh faktor lain yang tidak dimasukkan dalam penelitian ini.(1)

Banyak fasilitas yang disediakan oleh pihak perbankan untuk menunjang transaksi keuangan, dengan tujuan utama memberikan kemudahan bagi nasabah dalam bertransaksi. Selain layanan di cabang bank, tersedia pula fasilitas internet banking dan ATM. Saat ini, nasabah lebih cenderung menggunakan saluran pengiriman alternatif seperti ATM, internet banking, dan SMS banking untuk bertransaksi tanpa harus mengantri di bank. Dengan pertumbuhan transaksi online, penggunaan saluran pengiriman alternatif seperti perbankan online telah meningkat dan menjadi lebih populer.

A. Bidang Keamanan

seperti yang dijelaskan oleh Dony Ariyus, terdapat beberapa aspek dalam keamanan komputer, antara lain sebagai berikut:

1. *Authentication*: Memastikan bahwa penerima informasi dapat memverifikasi keaslian pesan dari pengirim.

2. *Integrity*: Memastikan keaslian pesan yang dikirimkan melalui jaringan dan bahwa informasi tersebut tidak diubah oleh pihak yang tidak berwenang.

3. *Non-repudiation*: Mengacu pada kemampuan pengirim untuk tidak menyangkal bahwa mereka telah mengirimkan pesan.

4. *Authority*: Mencegah pihak yang tidak berhak untuk mengubah atau memodifikasi informasi dalam sistem jaringan perbankan.

5. *Confidentiality*: Melindungi informasi dari akses yang tidak sah.

6. *Privacy*: Fokus pada perlindungan informasi pribadi.

7. *Availability*: Memastikan kesiapan informasi saat diperlukan.

8. *Access control*: Mengatur akses terhadap informasi. Alamat email wajib bagi penulis korespondensi (*corresponding author*). Keterangan

sebagai penulis korespondensi dituliskan setelah alamat email.

B. Sistem Keamanan pada Internet Banking

Untuk melindungi data nasabah, diperlukan kerjasama antara bank dan nasabah dalam menjaga sistem keamanan yang terkait dengan penggunaan layanan perbankan. Bank dapat mengambil langkah-langkah berikut untuk meningkatkan keamanan sistem perbankan:

1. *Sistem Kriptografi*: Sistem ini menggunakan angka yang dikenal sebagai kunci, sering disebut sebagai sistem kata sandi. Terdapat dua jenis metode enkripsi, yaitu simetris dan asimetris. Enkripsi simetris menggunakan kunci yang sama untuk penerima dan pengirim pesan, namun kelemahannya adalah kunci tersebut harus dikirim ke penerima, sehingga dapat diakses oleh pihak ketiga selama pengiriman. Enkripsi asimetris juga memiliki kelemahan, yaitu menurunnya kecepatan transfer data karena adanya kode tambahan. Sistem ini umumnya digunakan untuk mengidentifikasi nasabah dan melindungi informasi keuangan mereka.

2. *Firewall*: Firewall adalah sistem yang mencegah akses tidak sah ke area yang dilindungi dalam unit kerja perusahaan. Firewall berfungsi dengan menggandakan dan memperumit penghalang yang ada untuk mencegah pihak-pihak yang tidak berizin. Namun, perlu dicatat bahwa firewall tidak dapat sepenuhnya mencegah masuknya virus ke dalam sistem.

C. Peran konsumen dalam menjaga akun pribadi sangat penting dalam upaya pengamanan data konsumen. Nasabah dapat melakukan hal-hal berikut untuk meningkatkan keamanan sistem bank:

1. *Registrasi Perangkat*; teknik ini membatasi akses ke sistem perbankan melalui perangkat yang tidak dikenal atau tidak terdaftar di sistem. Perangkat ini mengidentifikasi pengguna melalui scan sidik jari.

2. *Completely Automated Public Turing Test to Tell Computers and Humans Apart (CAPTCHA)* adalah teknik baru yang diterapkan pada sistem perbankan

untuk mencegah serangan otomatis pada sesi atau halaman konfirmasi web. Metode ini memerlukan pengguna yang sah untuk memasukkan informasi dalam gambar atau audio secara acak, yang membuat program otomatis (robot otomatis) sulit untuk mengidentifikasi dan memproses informasi tersebut sebagai konfirmasi.

3. Dalam model Positif Identifikasi, klien bank diminta untuk memberikan informasi rahasia yang hanya diketahui klien tersebut dalam rangka untuk mengidentifikasi diri. Ini adalah pilihan kedua untuk otentikasi.

4. Salah satu metode pengamanan yang paling umum yang dapat digunakan pelanggan adalah username dan password. Sebelum mereka dapat mengakses akun mereka, pelanggan harus memasukan beberapa karakter untuk mengamankan akun mereka. Untuk masing-masing bank penyedia layanan, username dan password terdiri dari beberapa karakter. Beberapa bank juga menetapkan persyaratan khusus untuk jumlah dan jenis karakter yang digunakan untuk username dan password.

D. Contoh Jenis Serangan pada E-Banking

Beberapa ancaman hacking yang biasanya terjadi bertujuan untuk merusak sistem keamanan bank. Serangan ini menargetkan sistem perbankan dan kebiasaan penggunaan nasabah. Dalam pekerjaan keamanan, risiko tertinggi juga harus dipahami berdasarkan kepadatan jaringan dan besarnya dampak dari ancaman berikut. Berikut adalah beberapa jenis serangan terhadap sistem pelayanan bank:

1. *Brute Force Attack*: Teknik penyerangan terhadap sistem keamanan komputer ini menggunakan semua kemungkinan kombinasi kata sandi atau menggunakan kata sandi acak. Pendekatan ini melibatkan program yang mencoba berbagai kombinasi hingga menemukan kata sandi yang benar.

2. *Denial of Service (DoS) Attack*: Serangan ini berupaya menghalangi sistem target sehingga sistem tidak dapat memberikan layanan (denial of service). Metode serangan ini dapat bervariasi, dan

dampaknya juga berbeda-beda. Sistem yang diserang dapat mengalami kerusakan karena beban CPU yang tinggi, crash, atau penurunan kinerja sistem.

3. Virus, Worm, Trojan: Penyebaran virus, worm, atau Trojan bertujuan untuk mengganggu sistem komputer, mencuri informasi dari sistem korban, atau menyebabkan kerusakan pada sistem.

E. Dalam upaya pengamanan yang dilakukan, penting untuk memahami kemungkinan risiko tertinggi dari perspektif pola penggunaan layanan oleh pelanggan, seperti yang ditunjukkan oleh tingkat keseringan jaringan dan efek yang dihasilkan dari risiko. Serangan yang dapat terjadi dari sisi penggunaan sistem oleh pengguna didaftarkan di bawah ini:

1. DNS Hijacking adalah serangan keamanan jaringan komputer di mana seseorang dapat meletakkan dirinya di antara klien dan server DNS. Kemudian, penyerang dapat mengambil informasi klien dan mengirimkan kembali informasi yang salah ke klien sebelum informasi asli sampai ke server DNS. Kondisi menentukan kecepatan serangan ini. Jika penyerang ingin serangannya berhasil, dia harus membalas informasi klien sebelum informasi asli sampai ke server.

2. Phishing adalah serangan jarak jauh yang paling umum terhadap layanan keuangan online. Seorang penyerang menciptakan situs web yang hampir identik dengan situs web asli dan menggunakan alamat URL yang mirip dengan situs web aslinya, sehingga sulit untuk dicurigai. Selanjutnya, penyerang mengirimkan e-mail ke berbagai akun e-mail dengan konten yang mengarah pada alamat website palsu yang tersembunyi untuk diklik. Korban kemudian diyakinkan oleh penyerang bahwa mereka harus mengisi data karena ada perbaikan di server atau alasan lain yang menarik, dan mereka memberikan embel-embel berupa uang atau hadiah. Akibatnya, korban mengklik link palsu dan memberikan data pribadi mereka untuk layanan keuangan online tertentu, yang kemudian disalahgunakan oleh penyerang untuk mencuri.

3. typo site Pelaku menggunakan typosite untuk membuat nama situs palsu yang sama persis dengan situs asli dan alamat yang mirip dengan situs asli. Pelaku menunggu kesempatan jika seseorang korban salah mengetikkan alamat dan situs palsu yang dia buat. Jika hal ini terjadi, pelaku dapat dengan mudah mendapatkan data pengguna dan password korban dan menggunakannya untuk merugikan korban.

F. Kesalahan yang Dilakukan Nasabah: Meskipun berbagai metode perlindungan telah digunakan oleh bank dan nasabah, data nasabah masih dapat dicuri jika mereka sebagai pemilik akun melakukan kesalahan. Berikut ini adalah beberapa kesalahan yang paling sering dilakukan oleh pelanggan :

1. Ketika pelanggan ingin mengakses akun mereka, langkah pertama yang dihadapi mereka adalah password yang mudah ditebak, PIN, kata sandi, atau password. Orang-orang mungkin mengabaikan pentingnya menggunakan kata sandi yang aman. Beberapa pelanggan lebih suka menggunakan kombinasi karakter yang mudah diingat seperti 123456, 000000, abcdef, atau bahkan tanggal lahir mereka. Ini harus dihindari karena penggunaan kata sandi mudah ditebak.

2. Salah satu kelalaian pelanggan adalah jaringan internet yang tidak aman; mereka tidak memperhatikan jaringan internet yang mereka gunakan. Jika kita menggunakan jaringan internet yang tidak aman, orang lain dapat dengan mudah mencuri data kita. Dalam menggunakan internet, kita harus berhati-hati, terutama ketika kita berbagi jaringan internet dengan orang lain. Selain itu, VPN tidak direkomendasikan, terutama VPN yang tidak dapat dipertanggungjawabkan keamanannya.

3. Anti Virus Yang Kadaluarsa: Hampir semua anti virus dapat melindungi perangkat kita dari virus yang dapat mencuri data pribadi kita, tetapi anti virus yang telah kadaluarsa tidak dapat melindungi penggunanya lagi. Ini karena anti virus tersebut tidak dapat diupdate lagi.

4. Akun yang jarang diperiksa juga dapat diserang oleh hacker. Orang yang tidak memeriksa akunnya lagi tidak akan mendapatkan update atau

perkembangan terbaru. Hal ini juga dapat menyebabkan nasabah tidak mengetahui apa yang telah terjadi pada akunnya, entah itu dana masuk ke rekening atau penarikan dana yang nasabah sendiri tidak tahu.

G. Cara Pengamanan yang Perlu Dilakukan Nasabah: Berdasarkan ulasan tentang kesalahan yang sering dilakukan nasabah, berikut adalah cara yang perlu dilakukan nasabah untuk memperkuat akun sistem e-banking yang mereka gunakan:

1. **Pastikan Situs:** Pastikan pelanggan mengakses situs web yang benar. Pencuri seringkali mencoba mengirim pesan palsu yang menunjukkan alamat web yang mirip dengan alamat situs web asli bank yang ditiru.

2. **Mengganti kata sandi secara berkala,** gunakan kata sandi dan PIN yang tidak mudah ditebak, dan hindari menggunakan tanggal lahir sebagai PIN. Selain itu, pastikan untuk mengganti kata sandi secara berkala untuk menghindari orang yang tidak berkepentingan mengetahui kata sandi Anda.

3. **Ketika Anda ingin menggunakan I-banking,** gunakan selalu jaringan internet milik pribadi Anda. Hindari menggunakan jaringan yang digunakan bersama ketika Anda ingin menggunakan jaringan lain. Selain itu, pastikan jaringan yang digunakan bebas dari pengaruh pihak lain.
4. **Anti Virus Terupdate:** Pastikan anti virus perangkat selalu diupdate. Anti virus terupdate memiliki informasi terbaru tentang virus yang mungkin menyerang atau mencuri data.

IV. KESIMPULAN

Hasil penelitian tentang dampak sistem keamanan informasi perbankan terhadap pelanggan BRI yang menggunakan internet banking menunjukkan bahwa penerapan sistem keamanan informasi yang efektif dan canggih sangat penting untuk melindungi data dan transaksi nasabah dari berbagai ancaman keamanan siber. Beberapa komponen penting sistem keamanan termasuk autentikasi, integritas data, non-repudiation, otorisasi, kerahasiaan, privasi,

ketersediaan, dan kontrol transaksi. Oleh karena itu, peningkatan kesadaran dan perhatian terhadap keamanan data pengguna sangat penting untuk memberikan layanan perbankan online yang terpercaya dan aman.

Hasil penelitian ini menunjukkan bahwa peningkatan keamanan layanan internet banking dapat meningkatkan kepercayaan nasabah dan mengurangi risiko kejahatan siber yang dapat merugikan bank dan nasabah. Oleh karena itu, Bank Rakyat Indonesia (BRI) dan lembaga perbankan lainnya harus terus mengembangkan dan menerapkan teknologi keamanan siber yang paling canggih untuk menghadapi tantangan keamanan siber yang semakin kompleks. Sangat penting bagi pelanggan untuk dididik tentang praktik keamanan yang baik.

Melalui penelitian ini, disarankan agar Bank Rakyat Indonesia (BRI) dan lembaga keuangan lainnya meningkatkan upaya mereka untuk melindungi informasi pribadi dengan memperbarui teknologi, memperkuat kebijakan keamanan mereka, dan bekerja sama dengan spesialis keamanan siber. Perbankan dapat memastikan bahwa layanan perbankan online aman, terpercaya, dan memberikan keamanan terbaik bagi pelanggan mereka dengan langkah-langkah ini.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada semua pihak yang telah memberikan bantuan dan dukungan dalam penyelesaian penelitian ini. Ucapan terima kasih disampaikan kepada:

1. Bank Rakyat Indonesia (BRI) yang telah memberikan izin dan data yang diperlukan untuk penelitian ini.
2. Rekan-rekan di Teknik Informatika yang telah memberikan masukan berharga dan dukungan selama proses penelitian.
3. Dosen Pembimbing yang telah memberikan bimbingan, saran, dan koreksi selama penelitian ini berlangsung.
4. Keluarga dan teman-teman yang selalu memberikan dukungan moral dan motivasi.

Terima kasih juga kepada pihak-pihak lain yang tidak dapat disebutkan satu per satu, yang telah berkontribusi dalam penyusunan jurnal ini.

REFERENSI

- [1] Angga Pradana, and M. Irwan Padli Nasution. "Sistem Keamanan Informasi Perbankan pada Nasabah Pengguna Internet Banking." *JIKEM: Jurnal Ilmu Komputer, Ekonomi dan Manajemen* 2.2 (2022): 2739-2744.
- [2] Kusuma, A. P., & Nasution, M. I. P. (2022). Sistem Keamanan Informasi Perbankan pada Nasabah Pengguna Internet Banking. *JIKEM: Jurnal Ilmu Komputer, Ekonomi dan Manajemen*, 2(2), 2739-2744.
- [3] KUSUMA, Angga Pradana; NASUTION, M. Irwan Padli. Sistem Keamanan Informasi Perbankan pada Nasabah Pengguna Internet Banking. *JIKEM: Jurnal Ilmu Komputer, Ekonomi dan Manajemen*, 2022, 2.2: 2739-2744.
- [4] Safitri EM, Larasati AS. Analisis Keamanan Sistem Informasi E-Banking Di Era Industri 4.0: Studi Literatur. *J Ilm Teknol Inf dan Robot*. 2020;2(1):12–6.
- [5] Kamarudin J, Nursiah N, ... Pengaruh Faktor Kemudahan, Keamanan, dan Resiko Terhadap Kepuasan Nasabah Dalam Menggunakan Mobile Banking (Studi Kasus Pada Nasabah BRI Kabupaten Mamuju). *Forecast J Ilm Ilmu Manaj* [Internet]. 2022;1(2):11–8. Available from: <https://stiemmamuju.e-journal.id/FJIM/article/view/123%0Ahttps://stiemmamuju.e-journal.id/FJIM/article/download/123/63>
- [6] Wibowo Noor Fikri A, Fauzi A, Alfathur Rachman A, Khaerunisa A, Puspita Sari D, Vernanda P, et al. Analisis Keamanan Sistem Operasi dalam Menghadapi Ancaman Phishing dalam Layanan Online Banking. *J Ilmu Multidisplin*. 2023;2(1):84–91.
- [7] Kamarudin J, Nursiah N, ... Pengaruh Faktor Kemudahan, Keamanan, dan Resiko Terhadap Kepuasan Nasabah Dalam Menggunakan Mobile Banking (Studi Kasus Pada Nasabah BRI Kabupaten Mamuju). *Forecast J Ilm Ilmu Manaj* [Internet]. 2022;1(2):11–8. Available from: <https://stiemmamuju.e-journal.id/FJIM/article/view/123%0Ahttps://stiemmamuju.e-journal.id/FJIM/article/download/123/63>
- [8] Wibowo Noor Fikri A, Fauzi A, Alfathur Rachman A, Khaerunisa Puspita Sari D, Vernanda P, et al. Analisis Keamanan Sistem Operasi dalam Menghadapi Ancaman Phishing dalam Layanan Online Banking. *J Ilmu Multidisplin*. 2023;2(1):84–9
- [9] Maghfiroh, Widya Indah, et al. "Pengaruh e-service quality, e-trust dan e-satisfaction terhadap e-customer loyalty pada pengguna BRI Mobile (BRImo)." *SENTRI: Jurnal Riset Ilmiah* 1.2 (2022): 481-486.
- [10] Sinaga, Asmawarna, et al. "Penggunaan Fasilitas E-Banking Dalam Minat Nasabah Studi Kasus Pada PT. BRI Syariah Kantor Cabang Pembantu Stabat." *Journal Economy And Currency Study (JECS)* 3.2 (2021): 10-23.
- [11] Paniroi, Henry Fransisko, Erika Hardiyanti Kusuma Dewi, and Muhammad Irsad Khoiruddin. "M-banking: Layanan Jasa Bank dalam Mendapatkan Kepuasan Nasabah." *GLOBAL: Jurnal Lentera BITEP* 2.02 (2024): 63-68.
- [12] Hernandez, Axel, and Felix David. "Pengaruh Mobile Banking Terhadap Kepuasan Nasabah Bank Dalam Transaksi Sehari-Hari." *IT-Explore: Jurnal Penerapan Teknologi Informasi dan Komunikasi* 1.1 (2022): 17-32.
- [13] Pangestu, Putra Dena, et al. "JURNAL REVIEW: KONSEP KEAMANAAN PERBANKAN DI ERA DIGITAL." *HUMANITIS: Jurnal Homaniora, Sosial dan Bisnis* 2.7 (2024): 748-752.
- [14] Fikri, Adi Wibowo Noor, et al. "Analisis Keamanan Sistem Operasi dalam Menghadapi Ancaman Phishing dalam Layanan Online Banking." *Jurnal Ilmu Multidisplin* 2.1 (2023): 84-91.