

Analisis Serangan *Ransomware* Pada Sistem Keamanan Siber Bank Syariah Indonesia (BSI) Terhadap *Customer Trust*

Syam Muhaimin¹, Haslindah², Hasni³

^{1,2,3} Institut Agama Islam Negeri Bone, Jalan H.O.S Cokroaminoto, Watampone

Email: syammuhaimin55@gmail.com¹, putrileo0202@gmail.com², hasni.abdsalam@gmail.com³

Abstract: *The development of digital technology has brought significant benefits to the banking industry but has also increased cybersecurity risks, including the threat of ransomware attacks. Bank Syariah Indonesia (BSI) experienced a ransomware attack that affected its operational services and customer trust. This study aims to analyze the impact of the ransomware attack on customer trust at BSI Branch Bone. The research employs a descriptive qualitative approach, with data collected through interviews with customers. The findings indicate that the ransomware attack caused concern among customers, primarily due to delayed information and a lack of transparency from the bank in providing clarification regarding the incident. Most customers felt that BSI did not provide sufficiently detailed information about the impact of the attack on their data security, leading to a decline in trust in the bank. Therefore, this study recommends that BSI enhance its cybersecurity system, improve crisis communication strategies, and increase transparency in handling security incidents to maintain and restore customer trust.*

Keywords: *Cybersecurity, Customer Trust, Bank Syariah Indonesia*

Abstrak: Perkembangan teknologi digital membawa manfaat besar bagi industri perbankan, tetapi juga meningkatkan risiko keamanan siber, termasuk ancaman serangan ransomware. Bank Syariah Indonesia (BSI) mengalami insiden serangan ransomware yang berdampak pada operasional layanan dan kepercayaan nasabah. Penelitian ini bertujuan untuk menganalisis dampak serangan ransomware terhadap tingkat kepercayaan nasabah BSI Cabang Bone. Metode penelitian yang digunakan adalah pendekatan kualitatif deskriptif dengan teknik pengumpulan data melalui wawancara terhadap nasabah. Hasil penelitian menunjukkan bahwa serangan ransomware menyebabkan kekhawatiran di kalangan nasabah, terutama akibat keterlambatan informasi dan kurangnya transparansi dari pihak bank dalam memberikan klarifikasi mengenai insiden tersebut. Sebagian besar nasabah merasa bahwa BSI tidak memberikan informasi yang cukup rinci mengenai dampak serangan terhadap keamanan data mereka, yang mengakibatkan penurunan kepercayaan terhadap bank. Oleh karena itu, penelitian ini merekomendasikan agar BSI meningkatkan sistem keamanan siber, memperbaiki strategi komunikasi krisis, serta meningkatkan transparansi dalam menangani insiden keamanan untuk menjaga dan memulihkan kepercayaan nasabah.

Kata Kunci: Keamanan Siber, Kepercayaan Nasabah, Bank Syariah Indonesia

Pendahuluan

Dalam era digital, perbankan semakin mengadopsi teknologi informasi, namun juga menghadapi ancaman keamanan siber. Bank Syariah Indonesia (BSI) tidak luput dari risiko serangan, termasuk ransomware. Ransomware adalah malware yang mengenkripsi data pada sistem dan meminta tebusan untuk pemulihannya. Serangan ini berdampak serius pada bank karena melibatkan data sensitif nasabah, termasuk informasi keuangan dan identitas pribadi. Selain itu, ransomware dapat merusak reputasi bank dan menurunkan kepercayaan nasabah¹.

Kepercayaan merupakan sebuah kondisi dimana seseorang merasa hubungan emosional telah terbangun yang secara empiris telah terjalin dengan baik dengan mengesampingkan kemungkinan-kemungkinan yang dapat merusak hubungan emosional seseorang. Dalam konteks nasabah, maka kepercayaan nasabah merupakan sebuah kondisi dimana seorang nasabah sudah berani menyimpan atau menitipkan hartanya kepada bank tanpa ragu akan resiko yang bisa saja terjadi. Kepercayaan nasabah dikatakan sebagai pilar utama dalam kemajuan perbankan, untuk itu

¹ 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>.



lembaga perbankan perlu memiliki integritas agar supaya nasabah bisa memberikan rasa percayanya kepada bank itu sendiri. Kehilangan kepercayaan nasabah merupakan masalah serius bagi BSI, karena trust adalah kunci dalam perbankan. Jika nasabah merasa tidak aman, mereka dapat beralih ke layanan lain yang lebih andal. Oleh karena itu, penting untuk memahami dampak serangan ransomware terhadap kepercayaan nasabah BSI.²

Analisis data dari berbagai media menunjukkan perbedaan pernyataan terkait insiden yang dialami BSI. Hal ini wajar terjadi, terutama karena bank memiliki kepentingan untuk menjaga reputasi dan citranya. Pada 9 Mei 2023, melalui akun Instagram resminya, Manajemen BSI menyatakan bahwa gangguan layanan disebabkan oleh pemeliharaan sistem dan menyampaikan permintaan maaf atas ketidaknyamanan yang dialami nasabah.³ Namun, pernyataan ini menimbulkan pertanyaan, mengingat pemeliharaan sistem umumnya dilakukan pada hari libur dan bukan pada hari kerja, serta biasanya tidak berlangsung selama beberapa hari. Kondisi ini memicu dugaan bahwa penyebab gangguan bukan sekadar pemeliharaan sistem. Pada hari yang sama, akun Twitter @darktracer_int mengklaim bahwa kelompok peretas, yang diduga bernama LockBit 3.0, bertanggung jawab atas serangan terhadap BSI.⁴

Meningkatnya serangan siber di sektor keuangan menyoroti pentingnya perlindungan nasabah dari risiko seperti phishing, malware, dan gangguan layanan. Ancaman siber meningkat drastis hingga 86,70%, dengan IMF memperkirakan kerugian global sektor keuangan mencapai USD 100 miliar atau lebih dari Rp1.433 triliun per tahun.⁵ Kerentanan dalam mobile banking di Indonesia dapat menurunkan kepercayaan nasabah, yang berpengaruh pada citra bank. Kepercayaan nasabah berperan penting dalam keberlanjutan penggunaan layanan perbankan dan mempengaruhi loyalitas serta penerimaan pengguna di masa depan.⁶

Penelitian ini berfokus pada nasabah BSI Cabang Bone untuk menganalisis dampak serangan *ransomware* terhadap kepercayaan nasabah. Temuan dari penelitian sebelumnya oleh Lutfi Maulana dan Nadia Fitriana (2023) menunjukkan bahwa insiden serupa di BSI Kabupaten Subang berpengaruh signifikan terhadap tingkat kepercayaan (47,6%) dan loyalitas nasabah (35,6%).⁷ Insiden keamanan siber ini menimbulkan kekhawatiran terhadap kredibilitas BSI sebagai lembaga keuangan syariah. Oleh sebab itu Nasabah merupakan pilar utama yang mendukung keberlangsungan operasional bank, sehingga kepercayaan nasabah harus dijaga dengan baik. Penurunan kepercayaan dapat menyebabkan penurunan loyalitas, yang berdampak jangka panjang pada hubungan antara nasabah dan lembaga keuangan. Penulis menganggap bahwa setelah gangguan yang terjadi pada BSI menimbulkan beberapa pertanyaan dalam hal ini terkait akan kepercayaan dari nasabah tersebut serta tindakan yang dilakukan selanjutnya.

Penelitian ini bertujuan untuk mengevaluasi dampak serangan ransomware terhadap sistem keamanan siber BSI dan kepercayaan nasabahnya. Melalui analisis ini, diharapkan dapat

² Kementerian Agama RI, "Buku Saku Perbankan Syariah," 2013.

³ Agustinus Rangga Respati and Yoga Sukmana, "Perjalanan Kasus BSI, Dari Gangguan Layanan Sampai 'Hacker' Minta Tebusan," Kompas.com (Lhokseumawe, 2023), https://money.kompas.com/read/2023/05/17/072027926/perjalanan-kasus-bsi-dari-gangguan-layanan-sampai-hacker-minta-tebusan?page=all#google_vignette.

⁴ Nicky Maulana et al., "Manajemen Krisis PT. BSI Tbk Pasca Peretasan Data Nasabah," *INNOVATIVE: Journal Of Social Science Research* 4 (2024): 8244–58.

⁵ Dewi Fatmala Putri and Widya Ratna Sari, "Analisis Perlindungan Nasabah BSI Terhadap Kebocoran Data Dalam Menggunakan Digital Banking," *Jurnal Ilmiah Ekonomi Dan Manajemen* 1, no. 4 (2023): 173–81, <https://doi.org/10.61722/jiem.v1i4.331>.

⁶ Didik Setyawan et al., "Penguatan Kepercayaan Dalam Membentuk Niat Meneruskan Penggunaan Mobile Banking," *MBIA* 22 (May 19, 2023): 125–39, <https://doi.org/10.33557/mbia.v22i1.2291>.

⁷ Lutfi Maulana and Nadia Fitriana, "Analisis Dampak Insiden BSI Eror Dan Dugaan Hacking Bank Syariah Indonesia (BSI) Terhadap Kepercayaan Dan Loyalitas Nasabah Bank Syariah Indonesia Di Kabupaten Subang," *Jurnal Ilmu Islam* 7, no. 3 (2023): 1755–68.

diidentifikasi sejauh mana insiden ini mempengaruhi persepsi nasabah terhadap keamanan layanan perbankan. Metode penelitian meliputi pengumpulan data dari nasabah BSI Cabang Bone melalui survei dan wawancara guna memahami tingkat kepercayaan mereka terhadap bank setelah serangan terjadi. Hasil penelitian ini diharapkan dapat memberikan wawasan bagi BSI dalam meningkatkan keamanan siber dan menjaga kepercayaan nasabah.

Metode Penelitian

Jenis penelitian yang digunakan dalam penelitian ini adalah penelitian kualitatif dengan pendekatan yang digunakan adalah pendekatan deskriptif untuk melakukan analisis hanya sampai pada taraf deskriptif. Penelitian dilakukan di Kabupaten Bone Provinsi Sulawesi Selatan dengan waktu pelaksanaan dalam jangka dua bulan. Sata yang digunakan dalam penelitian ini berudpa data primer yang diperoleh secara langsung dari objek/subjek penelitian. Objek atau subjek penelitian ini adalah Nasabah dari Bank Syariah Indonesia (BSI) cabang Bone yang kemudian objek penelitiannya terkait tindakan dan dampak kepercayaan nasabah BSI Cabang Bone akibat dari serangan ransomware yang menyerang sistem keamanan Bank Syariah Indonesia (BSI). Adapun teknik pengumpulan data berupa wawancara dengan informan untuk mendapatkan informasi.⁸ Analisis data adalah proses sistematis dalam mengorganisir, menyusun, dan menyimpulkan data dari berbagai sumber agar lebih mudah dipahami.⁹ Teknik analisis data meliputi 3 tahap, yakni (1)Reduksi data, (2)Penyajian data, dan (3)Penarikan kesimpulan yang berupa temuan baru dari penelitian kualitatif.¹⁰

Hasil dan Pembahasan

1. Tanggapan Dan Dampak Kepercayaan Nasabah Bank Syariah Indonesia (BSI) Cabang Bone Terhadap Serangan Ransomware Yang Terjadi Pada BSI

a. Waktu tanggapan terhadap pemberitahuan

Hasil wawancara menunjukkan bahwa komunikasi BSI terkait insiden serangan siber dinilai lambat, kurang transparan, dan tidak mendetail. Andi Hardiyanti Nur dan Asmar Hidayat kecewa karena baru mengetahui insiden ini melalui email atau media sosial beberapa hari setelahnya. Sebaliknya, Bapak Andi Geerhand dan Bapak Ibrahim menerima pemberitahuan lebih cepat melalui aplikasi BSI Mobile, tetapi tetap menilai informasi yang diberikan terlalu umum dan kurang menjelaskan detail kejadian.

Sebagian besar nasabah tetap khawatir akan keamanan data mereka. Bapak Riswan Rusli dan Bapak Ibrahim menyoroti kurangnya kejelasan dalam klarifikasi BSI, sementara Bapak Andi Geerhand mengkritik minimnya informasi mengenai penyebab dan dampak insiden. Kurangnya transparansi ini memicu spekulasi dan menurunkan kepercayaan nasabah, seperti yang dialami Andi Hardiyanti Nur, Asmar Hidayat, dan Riswan Rusli. Meskipun demikian, beberapa nasabah, seperti Bapak Ibrahim, masih mempertahankan kepercayaan mereka tetapi mengharapkan transparansi yang lebih baik di masa depan.

b. Penerimaan dan penolakan terhadap penjelasan BSI

Hasil wawancara mengungkapkan bahwa mayoritas nasabah menilai penjelasan BSI terkait serangan siber kurang transparan dan tidak cukup detail, sehingga menimbulkan spekulasi dan kekhawatiran. Andi Hardiyanti Nur dan Asmar Hidayat

⁸ Feny Rita Fiantika Mohammad Wasil Sri Jumiyati Leli Honesti Sri Wahyuni et al., *Metodologi Penelitian Kualitatif*, Rake Sarasin, 1st ed. (Padang: PT. Global Eksekutif Teknologi, 2020).

⁹ Ahmad Andreas et al., *Metodologi Penelitian* (Padang: CV. Gita Lentera, 2024).

¹⁰ Ahmad Rijali, "Analisis Data Kualitatif," *Alhadharah: Jurnal Ilmu Dakwah* 17, no. 33 (2019): 81, <https://doi.org/10.18592/alhadharah.v17i33.2374>.

merasa informasi yang diberikan tidak memadai, bahkan menduga adanya fakta yang disembunyikan, yang semakin mengurangi kepercayaan mereka.

Bapak Riswan Rusli dan Bapak Ibrahim menganggap penjelasan BSI terlalu umum dan tidak menjelaskan langkah konkret dalam melindungi data nasabah, sehingga mereka tetap meragukan keamanannya. Sementara itu, Bapak Andi Geerhand menilai bahwa meskipun BSI telah memberikan gambaran umum, transparansi lebih lanjut tetap dibutuhkan agar nasabah memahami risiko dan dapat mengambil tindakan perlindungan yang tepat.

c. Keterlibatan dalam proses pemulihan

Temuan wawancara menunjukkan bahwa keterlibatan nasabah dalam proses pemulihan setelah serangan siber terhadap BSI masih minim, dengan kurangnya arahan jelas mengenai langkah pengamanan akun. Andi Hardiyanti Nur dan Asmar Hidayat merasa tidak mendapat instruksi resmi dan harus mengambil inisiatif sendiri untuk mengganti kata sandi, sementara Bapak Riswan Rusli baru mengganti kata sandi setelah membaca berita, bukan berdasarkan arahan BSI. Bapak Andi Geerhand dan Bapak Ibrahim mengikuti rekomendasi BSI, seperti mengganti kata sandi dan mengaktifkan autentikasi dua faktor, tetapi tetap menganggap informasi yang diberikan kurang mendalam. Mereka berharap adanya panduan yang lebih terperinci, seperti tutorial atau notifikasi yang lebih jelas terkait langkah keamanan tambahan.

d. Pengaruh terhadap loyalitas layanan

Temuan wawancara dalam penelitian ini mengungkap bahwa insiden serangan siber berdampak signifikan terhadap loyalitas nasabah BSI, dengan banyak yang mengalami penurunan kepercayaan dan mempertimbangkan untuk beralih ke bank lain. Andi Hardiyanti Nur dan Asmar Hidayat secara tegas menyatakan ketidakpuasan mereka terhadap respons BSI yang dinilai kurang cepat dan sistem keamanannya yang belum cukup dapat diandalkan.

Sementara itu, Andi Geerhand dan Ibrahim masih loyal terhadap BSI, tetapi menuntut perbaikan sistem keamanan dan peningkatan transparansi agar kepercayaan mereka tetap terjaga. Riswan Rusli menyatakan keraguannya untuk tetap menggunakan layanan BSI, menekankan bahwa keamanan adalah prioritas utama dalam memilih bank, dan ia akan mencari alternatif lain jika perbaikan tidak segera dilakukan.

e. Perubahan dalam Persepsi Reputasi BSI

Wawancara dengan beberapa nasabah BSI mengindikasikan bahwa insiden yang terjadi berdampak negatif terhadap reputasi bank, dengan banyak nasabah mengalami penurunan kepercayaan. Andi Hardiyanti Nur dan Asmar Hidayat meragukan kemampuan BSI untuk memulihkan citranya tanpa adanya langkah konkret yang transparan dan efektif. Sementara itu, Andi Geerhand dan Ibrahim masih optimis bahwa reputasi bank dapat dipulihkan melalui perbaikan sistem keamanan dan komunikasi yang lebih baik. Dengan demikian, pemulihan kepercayaan nasabah bergantung pada sejauh mana BSI dapat meningkatkan transparansi serta mengambil langkah strategis dalam memperkuat keamanannya.

2. Sikap dan tindakan nasabah Bank Syariah Indonesia (BSI) Cabang Bone terhadap serangan ransomware yang terjadi pada BSI

a. Tingka kecemasan atau ketidakpercayaan

Serangan siber yang menimpa BSI pada Mei 2023 berdampak signifikan terhadap kepercayaan nasabah, terutama akibat kurangnya komunikasi dan transparansi dari pihak bank. Banyak nasabah mengalami kepanikan karena tidak dapat mengakses rekening mereka melalui aplikasi mobile banking. Andi Hardiyanti Nur, misalnya, merasa cemas terhadap keamanan saldonya dan berusaha mencari informasi melalui media sosial, namun justru menemukan berita simpang siur yang semakin memperburuk kekhawatirannya. Ketidakmampuan layanan pelanggan BSI dalam memberikan jawaban yang jelas semakin menambah ketidakpastian di kalangan nasabah.

Kepercayaan nasabah terhadap bank sangat bergantung pada kecepatan dan keterbukaan komunikasi, terutama dalam situasi krisis. Untuk memulihkan kepercayaan

tersebut, BSI perlu meningkatkan transparansi dalam menyampaikan informasi, memperbaiki sistem keamanannya, serta memberikan respons yang lebih cepat terhadap keluhan nasabah. Dengan langkah-langkah ini, diharapkan nasabah dapat kembali merasa aman dan yakin bahwa BSI mampu melindungi data serta dana mereka secara optimal.

b. Persepsi terhadap tindakan BSI

Kesimpulan dari wawancara dengan para nasabah BSI menunjukkan bahwa mayoritas merasa kurang puas dengan respons bank terhadap serangan ransomware yang terjadi. Andi Hardiyanti Nur dan Andi Geerhand mengkritik lambatnya klarifikasi dan pemulihan layanan, sementara Asmar Hidayat menyoroti perlunya sistem cadangan dan kompensasi bagi nasabah terdampak. Riswan Rusli mengakui upaya BSI dalam menangani insiden ini tetapi berharap respons yang lebih cepat, sedangkan Ibrahim menekankan pentingnya kesiapan bank dalam menghadapi serangan siber di masa depan.

Secara umum, para nasabah menuntut transparansi lebih baik, peningkatan sistem keamanan, serta solusi yang lebih cepat dalam menangani gangguan layanan. Kejadian ini menjadi pelajaran bahwa bahkan lembaga keuangan besar pun tidak luput dari ancaman siber, sehingga diperlukan langkah-langkah strategis untuk memulihkan kepercayaan nasabah dan mencegah insiden serupa di masa mendatang.

Kepuasan terhadap Komunikasi BSI

Dari hasil wawancara beberapa narasumber dapat disimpulkan bahwa terdapat permasalahan serius terkait sistem komunikasi Bank Syariah Indonesia (BSI) saat menangani insiden. Lambatnya penyampaian informasi dan kurangnya transparansi dari pihak bank telah memicu kepanikan di antara para nasabah. Situasi ini menunjukkan adanya kebutuhan mendesak untuk memperbaiki strategi komunikasi BSI, di mana nasabah mengharapkan sistem yang lebih responsif yang dapat menyediakan informasi secara real-time, dengan tingkat akurasi yang tinggi, dan dapat diakses dengan mudah oleh semua nasabah.

c. Penggunaan layanan yang berhati-hati

Insiden serangan siber terhadap BSI mendorong nasabah seperti Andi Hardiyanti Nur, Asmar Hidayat, Andi Geerhand, Riswan Rusli, dan Ibrahim untuk lebih waspada dalam menjaga keamanan akun perbankan mereka. Berbagai langkah preventif dilakukan, seperti yang dilakukan oleh Andi Hardiyanti Nur yang segera mengganti password mobile banking, mengaktifkan notifikasi transaksi, dan lebih sering mengecek saldo. Asmar Hidayat meningkatkan keamanan dengan autentikasi dua faktor serta lebih berhati-hati terhadap tautan mencurigakan. Sementara itu, Andi Geerhand lebih mengandalkan SMS banking dan rutin memeriksa mutasi rekening, sedangkan Riswan Rusli lebih aktif memantau aktivitas rekeningnya serta mengganti password dan PIN ATM. Ibrahim juga menekankan pentingnya verifikasi dua langkah untuk meningkatkan perlindungan terhadap akun perbankannya.

Langkah-langkah ini mencerminkan peningkatan kesadaran nasabah terhadap pentingnya perlindungan data perbankan setelah insiden terjadi. Ke depannya, konsistensi dalam menerapkan langkah-langkah keamanan, serta edukasi yang lebih baik dari pihak bank mengenai keamanan digital, menjadi faktor penting dalam menjaga kepercayaan nasabah dan mengurangi risiko serangan siber di masa mendatang.

Kesimpulan

Berdasarkan hasil penelitian, dapat disimpulkan bahwa serangan *ransomware* terhadap BSI berdampak signifikan pada kepercayaan nasabah yakni:

1. Dampak Keamanan Siber

- a. Serangan ransomware menyebabkan gangguan layanan yang berdampak pada operasional perbankan, menghambat akses nasabah terhadap layanan keuangan mereka.
- b. Keterlambatan dalam pemberian informasi serta kurangnya transparansi dalam komunikasi memperburuk kondisi kepercayaan nasabah terhadap BSI.

2. Respon Nasabah

- a. Mayoritas nasabah merasa bahwa pemberitahuan dari BSI terkait insiden ini terlambat dan tidak memberikan penjelasan yang cukup detail mengenai dampak serta langkah mitigasi yang diambil.
 - b. Beberapa nasabah mengalami penurunan tingkat kepercayaan terhadap bank karena kekhawatiran akan keamanan data pribadi dan kejelasan tanggung jawab BSI terhadap insiden tersebut.
3. Keterbukaan dan Transparansi
- a. Kurangnya transparansi dalam menangani insiden ini membuat beberapa nasabah merasa skeptis terhadap sistem keamanan yang dimiliki oleh BSI.
 - b. Meskipun sebagian nasabah masih mempertahankan kepercayaan terhadap BSI, mereka tetap menginginkan peningkatan transparansi dan langkah-langkah perlindungan yang lebih baik untuk menghindari kejadian serupa di masa depan.

Daftar Pustaka

- Andreas, Ahmad, Andreas Tri Panudju, Febriani Purba, Erlina, Salis Nurbaiti, Yolan Septaria, Septaria Kalalinggi, et al. *Metodologi Penelitian*. Padang: CV. Gita Lentera, 2024.
- Fatmala Putri, Dewi, and Widya Ratna Sari. "Analisis Perlindungan Nasabah BSI Terhadap Kebocoran Data Dalam Menggunakan Digital Banking." *Jurnal Ilmiah Ekonomi Dan Manajemen* 1, no. 4 (2023): 173–81. <https://doi.org/10.61722/jiem.v1i4.331>.
- 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>.
- Kementerian Agama RI. "Buku Saku Perbankan Syariah," 2013.
- Maulana, Lutfi, and Nadia Fitriana. "Analisis Dampak Insiden BSI Error Dan Dugaan Hacking Bank Syariah Indonesia (BSI) Terhadap Kepercayaan Dan Loyalitas Nasabah Bank Syariah Indonesia Di Kabupaten Subang." *Jurnal Ilmu Islam* 7, no. 3 (2023): 1755–68.
- Maulana, Nicky, Tito Laurens, Hadrian Afzal Faiz, and Tria Patrianti. "Manajemen Krisis PT. BSI Tbk Pasca Peretasan Data Nasabah." *INNOVATIVE: Journal Of Social Science Research* 4 (2024): 8244–58.
- Respati, Agustinus Rangga, and Yoga Sukmana. "Perjalanan Kasus BSI, Dari Gangguan Layanan Sampai 'Hacker' Minta Tebusan." Kompas.com. Lhokseumawe, 2023. https://money.kompas.com/read/2023/05/17/072027926/perjalanan-kasus-bsi-dari-gangguan-layanan-sampai-hacker-minta-tebusan?page=all#google_vignette.
- Rijali, Ahmad. "Analisis Data Kualitatif." *Alhadharah: Jurnal Ilmu Dakwah* 17, no. 33 (2019): 81. <https://doi.org/10.18592/alhadharah.v17i33.2374>.
- Setyawan, Didik, Vincentia Damayanti, Sugiyarmasto Sugiyarmasto, and Nang Budiadi. "Penguatan Kepercayaan Dalam Membentuk Niat Meneruskan Penggunaan Mobile Banking." *MBIA* 22 (May 19, 2023): 125–39. <https://doi.org/10.33557/mbia.v22i1.2291>.
- Wahyuni, Feny Rita Fiantika Mohammad Wasil Sri Jumiyati Leli Honesti Sri, Erland Mouw Jonata, Imam Mashudi Nur Hasanah, Anita Maharani, Kusmayra Ambarwati Resty Noflidaputri Nuryami, and Lukman Waris. *Metodologi Penelitian Kualitatif*. Rake Sarasin. 1st ed. Padang: PT. Global Eksekutif Teknologi, 2020.