JOURNAL SYNTAX IDEA
p–ISSN: 2723-4339 e-ISSN: 2548-1398
Vol. 5, No. 7, Juli 2023

MENDESAIN *CYBER SECURITY CORE BANKING SYSTEM* UNTUK KEAMANAN MENGGUNAKAN *FIREWALL* PADA PT. BANK SYARIAH INDONESIA TBK

Muhammad Kevin Meidiandra, Yulia Permata Sari, Tata Sutabri
Magister Teknik Informatika, Universitas Bina Darma Palembang
Email: yuliapermatasari44@gmail.com, kevinawalludin@gmail.com, tata.Sutabri@binadarma.ac.id

Abstract

Teknologi yang semakin canggih layanan perbankan dapat memberikan kemudahan nasabah dalam bertransaksi. Dengan hasil yang telah kami teliti bahwa jaringan dengan menggunakan firewall memiliki beberapa tahap yaitu identifikasi aktivasi dan ancaman, pemilian jenis firewall, segmentasi jaringan, uji keamanan dan simulasi serangan, dan evaluasi dan perbaikka. Dalam hal tersebut bank syariah Indonesia dapat meningkatkan tingkat keamanan cyber dengan menggunakan firewall sebagai salah satu lapisan pertahanan kritis dalam infrastruktur IT mereka agar dapat melindungi ancaman cyber dan teknologi keamanan untuk menjaga sistem tetap aman.

Keywords: Cyber, Firewall, Core Banking

PENDAHULUAN

Teknologi Informasi sudah merupakan suatu kebutuhan yang sangat penting, bahkan sebagai tuntunan yang mendesa bagi setiap orang untuk menyelesaikan semua permasalahan dengan cepat serta meringankan semua pekerjaannya (Sari & Sutabri, 2023). Seiring dengan situasi seperti ini perkembangan teknologi informasi terutama peranan komputer mendapatkan perhatian yang sangat serius (Antoni, 2017). Teknologi informasi ini memberi dampak luar biasa dalam dunia perbankan saat ini.

Layanan perbankan untuk transaksi keuangan banyak memberikan kemudahan nasabah dalam bertransaksi. Selain pelayananan di kantor bank, terdapat layanan menggunakan internet banking dan juga Atm (Hukum & RI, 2004). Tingginya kebutuhan akan bertransaksi yang mudah, aman dan cepat menuntut setiap bank meningkatkan pelayanan khususnya dibidang kemanan *cyber securty*, agar dapat menjawab tantangan saat ini berupa *cybercrime* (Mangadil, 2016).

Penggunaan intenet tidak hanya terbatas pada pemnfaatan informasi yang dapat diakses melalui media, melainkan juga dapat digunakan sebagai sarana untuk melakukan

How to cite: Muhammad Kevin Meidiandra, Yulia Permata Sari, Tata Sutabri (2023), Mendesain Cyber Security Core Banking System untuk Keamanan Menggunakan Firewall Pada PT. Bank Syariah Indonesia Tbk, *(5) 7,* https://doi.org/10.46799/syntax-idea.v5i7.2416 __
E-ISSN: 2684-883X
Published by: Ridwan Institute

transaksi perbankan (Firmansyah, 2017). Sebagai sarana untuk melakukan transaksi perbankan bank Indonesia mulai memasuki dunia maya yaitu internet *e-banking* yang merupakan bentuk layanan perbankan secara elekctronik melalui media e-bangking pada dasarnya merupakan suatu kontrak transaksi antara pihak bank dan nasabah yang memberikan manfaat berganda dengan menggunakan media internet (Sutabri, 2014). Transaksi perbankan dapat dilakukan dimana saja dan kapan saja tanpa dibatasi tempat dan waktu, semakin relavannya teknologi internet didunia perbankan.

Melihat hal tersebut maka Bank Syariah Indonesia Tbk mencoba menjaring nasabah dan mempertahankan nasabah dengan meluncurkan suatu fasilitas internet *core banking* (Sutabri, 2012). Penggunaan Internet Banking ini diharapkan dapat memenuhi kebutuhan layanan yang baik bagi nasabah, dengan dukungan SDM Perbankan yang profesional serta kemampuan menguasai dan melayani nasabah dengan produk- produk inovatif tersebut.

Strategi untuk menghadapi persaingan dalam dunia perbankan pada umumnya serta sebagai peningkatan mutu layanan kepada nasabah pada khususnya, maka dengan ini penulis akan membahas *security* untuk keamanan *internet core banking* pada bank syariah Indonesia tbk sebagai salah satu pemenuhan tanggung jawab Mandiri dalam memberikan layanan yang unggul yang di terapkan oleh Bank Syariah Indonesia tbk, dan kami menetapkan **" Mendesain *cyber security* untuk keamanan *core bangking system* menggunakan *Firewall* pada PT. Bank Syariah Indonesia Tbk"** sebagai tema dan sekaligus menjadi judul Uas dalam penyusunan *paper* ini.

Internet Banking kini bukan lagi istilah yang asing bagi masyarakat Indonesia khususnya yang tinggal di wilayah perkotaan (Khasanah & Sutabri, 2023; Puntoadi, 2011). Hal tersebut disebabkan semakin banyaknya perbankan nasional yang menyelenggarakan layanan tersebut. Di masa mendatang, layanan ini tampaknya sudah bukan lagi sebuah layanan yang akan memberikan *competitive advantage* bagi bank yang menyelenggarakannya. Keadaannya akan sama seperti pemberian fasilitas ATM. Semua bank akan menyediakan fasilitas tersebut.

Penyelenggaraan Internet Banking yang sangat dipengaruhi oleh perkembangan teknologi informasi, dalam kenyataannya pada satu sisi membuat jalannya transaksi perbankan semakin mudah, akan tetapi di sisi yang lain membuatnya juga semakin berisiko. Dengan kenyataan seperti ini, faktor keamanan harus menjadi faktor yang paling perlu diperhatikan. Bahkan mungkin faktor keamanan ini dapat menjadi salah satu fitur unggulan yang dapat ditonjolkan oleh pihak bank. Diskusi ini mencoba mengidentifikasi berbagai permasalahan tersebut dan alternatif pemecahannya.

METODE PENELITIAN

Metode penelitian yang dipakai dalam penelitian ini adalah Metode *Firewall* dimana ada beberapa tahap dalam penelitian tersebut.

1. Analisa kebutuhan

   Pada Bank Syariah Indonesia tbk teknologi solusi membutuhkan *system* keamanan *security* yang lebih ketat agar dapat menjaga keamanan *core banking system*, dengan

menangkal serangan dari pihak sketiga, membatasi akses internal yang berpotensi menyebabkan serangan atau hal yang berdampak negative bagi user internal dan meninjau *traffic* di berbagai *platform* pada jaringan tersebut.

2. Desain
   Penulis akan melakukan perancangan desain keamanan security pada *core banking system* dengan menggunakan *software cisco packet tracer* untuk menggambarkan skema jaringan yang diusulkan dengan membuat topologi keamanan *security*.

HASIL DAN PEMBAHASAN

Merencanakan Jaringan Dengan *Firewall*

Merencanakan kemanan jaringan dengan *firewall* memiliki beberapa tahapan, beberapa diantaranya adalahh (Jayanti et al., 2016):

- Identifikasi Aktivasi dan Ancaman
  Pada tahapan ini akan ditentukan jenis data sensitif yang harus dilindungi oleh firewall, serta ancaman yang paling mungkin dihadapi oleh bank. Ini dapat mencakup informasi keuangan, data pribadi nasabah, transaksi, dan lainnya.
- Pemilihan Jenis Firewall
  Pada tahap ini dilakukan pemilihan jenis firewall yang sesuai dengan kebutuhan bank syariah indonesia. Apakah akan digunakan firewall perangkat keras, perangkat lunak, atau solusi firewall berbasis cloud tergantung pada arsitektur jaringan dan kebutuhan keamanan.
- Segmentasi Jaringan
  Bagi jaringan internal bank menjadi zona atau segmen yang berbeda sesuai dengan tingkat keamanan dan fungsi. Misalnya, zona untuk nasabah, zona untuk karyawan, dan zona untuk server. Ini membantu mencegah penyebaran potensial dari serangan.
- Uji Keamanan dan Simulasi Serangan
  Pada tahap ini akan dilakukan uji penetrasi secara berkala untuk mengidentifikasi kerentanan dan memastikan bahwa firewall serta sistem keamanan lainnya dapat melindungi dari serangan yang mungkin terjadi.
- Evaluasi dan Perbaikan
  Tahap akhir yang juga sangat penting adalah evaluasi dan perbaikan dimana terus diperhatikan aspek aspek yang belum memenuhi harapan dari keamanan sistem pada Bank Syariah Indonesia

Optimalisasi Jaringan dengan *Firewall*

Optimalisasi keamanan cyber dengan menggunakan firewall sangat penting bagi bank Syariah Indonesia atau lembaga keuangan mana pun. Firewall adalah salah satu komponen kunci dalam pertahanan siber yang membantu melindungi sistem dan data dari ancaman yang berasal dari internet (Djanggih & Qamar, 2018). Di bawah ini adalah beberapa langkah yang dapat diambil untuk optimalisasi keamanan cyber dengan firewall pada Bank Syariah Indonesia:

- Pemahaman Kebutuhan: Identifikasi kebutuhan keamanan yang spesifik untuk bank Syariah. Ini mungkin termasuk regulasi yang harus diikuti, jenis data sensitif yang harus dilindungi, dan jenis ancaman yang mungkin dihadapi.
- Pemilihan Jenis Firewall: Pilih jenis firewall yang sesuai dengan kebutuhan bank. Ada dua jenis utama: firewall perangkat keras dan firewall perangkat lunak. Firewall perangkat keras lebih tangguh dan mampu menangani beban kerja yang lebih berat, sementara firewall perangkat lunak lebih fleksibel.
- Segmentasi Jaringan: Pisahkan jaringan internal bank menjadi zona-zona yang berbeda dan terlindungi oleh firewall. Ini membantu mencegah penyebaran malware dari satu bagian jaringan ke bagian lain.
- Konfigurasi yang Ketat: Konfigurasikan firewall dengan aturan yang ketat dan sesuai dengan kebijakan keamanan bank. Batasi lalu lintas jaringan hanya pada layanan dan protokol yang benar-benar diperlukan untuk operasi bisnis.
- Monitoring dan Pelaporan: Pasang sistem monitoring yang kuat untuk melacak lalu lintas jaringan dan mendeteksi aktivitas mencurigakan. Setel notifikasi dan pelaporan untuk memberi tahu tim keamanan tentang potensi ancaman.
- Pembaruan Rutin: Pastikan firewall selalu diperbarui dengan versi perangkat lunak terbaru dan definisi ancaman terbaru. Ini akan membantu melindungi jaringan dari kerentanan yang telah ditemukan dan dieksploitasi oleh penyerang.
- Pengujian Keamanan: Lakukan pengujian penetrasi dan audit keamanan secara berkala untuk mengidentifikasi kerentanan yang mungkin ada dalam sistem dan infrastruktur IT bank.
- Pendidikan Karyawan: Lakukan pelatihan keamanan siber untuk karyawan bank, terutama mereka yang memiliki akses ke jaringan internal. Kesadaran tentang ancaman siber dan praktik keamanan yang baik dapat mengurangi risiko serangan.
- Backup dan Pemulihan Bencana: Selain firewall, pastikan ada strategi pemulihan bencana yang baik. Cadangkan data secara teratur dan simpan cadangan di lokasi yang aman, terpisah dari jaringan utama.
- Tim Keamanan Cyber: Bentuk tim keamanan siber yang akan memantau dan mengelola infrastruktur keamanan, merespons insiden, dan mengembangkan kebijakan keamanan yang diperlukan.
- Kebijakan Keamanan: Tetapkan kebijakan keamanan yang jelas dan tegas. Pastikan semua karyawan memahami dan mengikuti pedoman keamanan ini.
- Kerjasama dengan Penyedia Keamanan: Bekerja sama dengan penyedia layanan keamanan siber terkemuka untuk mendapatkan informasi tentang ancaman terbaru dan solusi keamanan inovatif.

Dengan mengambil langkah-langkah ini, bank Syariah Indonesia dapat meningkatkan tingkat keamanan cyber dengan menggunakan firewall sebagai salah satu lapisan pertahanan kritis dalam infrastruktur IT mereka. Penting untuk selalu beradaptasi

dengan perubahan dalam ancaman siber dan teknologi keamanan terbaru untuk menjaga sistem tetap aman.

KESIMPULAN

Pada era saat ini tentunya perancangan keamanan siber dengan penerapan *firewall* pada Bank Syariah Indonesia dengan langkah-langkah yang telah diambil merupakan komponen kritis dalam memastikan integritas, kerahasiaan, dan ketersediaan data serta *infrastruktur* teknologi. Dalam era di mana ancaman siber semakin kompleks dan meresahkan, perlindungan terhadap informasi nasabah, data transaksi keuangan, dan operasional bank menjadi prioritas utama.

Penerapan *firewall* pada lingkungan jaringan bank merupakan solusi yang efektif dalam memerangi berbagai bentuk serangan siber seperti malware, peretasan, serta upaya mencuri data sensitif. Dengan merancang aturan-aturan yang tepat dan memisahkan segmen jaringan, bank dapat mengurangi risiko penyebaran serangan dan potensial kerugian akibat insiden keamanan.

Dengan adanya perancangan keamanan siber yang kokoh, termasuk penggunaan firewall yang tepat, Bank Syariah Indonesia dapat memberikan keyakinan kepada nasabahnya bahwa informasi mereka aman dan dilindungi. Dalam menjalankan misi sebagai institusi keuangan yang terpercaya, perencanaan keamanan siber menjadi salah satu pilar utama dalam menjaga reputasi, kepercayaan, dan kelangsungan operasional bank

BLIBLIOGRAFI

Antoni, A. (2017). Kejahatan Dunia Maya (Cyber Crime) Dalam Simak Online. *Nurani: Jurnal Kajian Syari'ah Dan Masyarakat*, *17*(2), 261–274.

Djanggih, H., & Qamar, N. (2018). Penerapan Teori-Teori Kriminologi dalam Penanggulangan Kejahatan Siber (Cyber Crime). *Pandecta Research Law Journal*, *13*(1), 10–23.

Firmansyah, R. (2017). Web klarifikasi berita untuk meminimalisir penyebaran berita hoax. *Jurnal Informatika*, *4*(2).

Hukum, P., & RI, P. M. A. (2004). *Naskah Akademis Kejahatan Internet (cybercrime)*.

Jayanti, L., Sentinuwo, S. R., Lantang, O. A., & Jacobus, A. (2016). Analisa Pola Penyalahgunaan Facebook Sebagai Alat Kejahatan Trafficking Menggunakan Data Mining. *Jurnal Teknik Informatika*, *8*(1).

Khasanah, N., & Sutabri, T. (2023). Analisis Kejahatan Cybercrime Pada Peretasan Dan Penyadapan Aplikasi Whatsapp. *Blantika: Multidisciplinary Journal*, *2*(1), 44–55.

Mangadil, D. M. (2016). Dampak Yuridis Penggunaan Media Sosial Menurut Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektonik. *Lex Et Societatis*, *4*(1).

Puntoadi, D. (2011). *Menciptakan Penjualan via Social Media*. Elex Media Komputindo.

Sari, Y. P., & Sutabri, T. (2023). Analisis Penyalagunaan Media Sosial Dalam Penyebaran Konten Di Aplikasi Facebook Mengunakan Metode Semi Deskriptif Kuantitatif. *Jursima (Jurnal Sistem Informasi Dan Manajemen)*, *11*(1), 212–216.

Sutabri, T. (2012). *Analisis sistem informasi*. Penerbit Andi.

Sutabri, T. (2014). Teknologi Informasi. *ANDI: Yogyakarta*.